PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-158654
(43)Date of publication of application : 31.05.2002

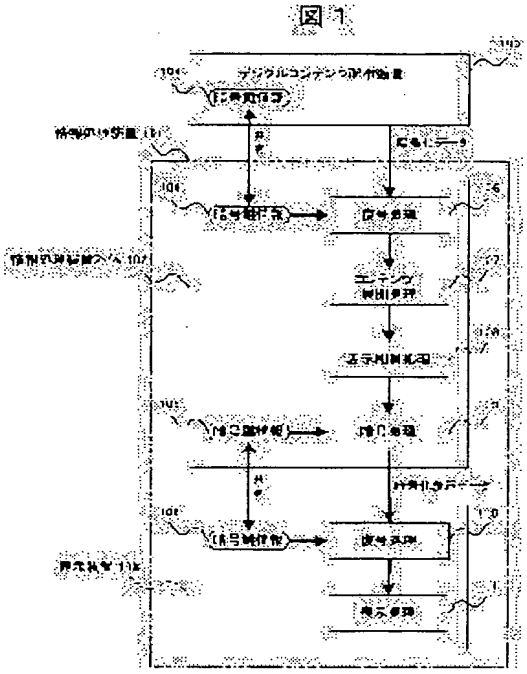
(51)Int.Cl. H04L 9/16
H04L 9/08
H04N 7/167

(21)Application number : 2000-351510
(22)Date of filing : 17.11.2000

(71)Applicant : HITACHI LTD
(72)Inventor : OWADA TORU
KITAHARA JUN
ASAHI TAKESHI

(54) INFORMATION PROCESSOR, DISPLAY DEVICE, DIGITAL CONTENTS DISTRIBUTION SYSTEM AND DIGITAL CONTENTS DISTRIBUTION/ OUTPUT METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To enable the final output of digital contents in a form to stimulate audio and visual desires of a user, while protecting rights of the digital contents.
SOLUTION: An information processor body 102 transfers the digital contents (display data) encoded by using an encoding key information 105 to be shared with a display device 103 to the display device 103 and the display device 103 performs a decoding processing to the display data to be transferred from the information processor body 102 by using the encoding key information 105. The display data to be transferred from the information processor body 102 to the display device 103 here is one, the only a part of which is encoded, for example, and every piece of display data for several lines is encoded every several lines.



LEGAL STATUS

[Date of request for examination] 28.01.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] In the information processor equipped with the processor and the output unit at least the above-mentioned processor A cipher-processing means to perform cipher processing to a digital content using the cryptographic key information shared with the above-mentioned output unit, It has a transfer means to transmit the enciphered digital content to the above-mentioned output unit. The above-mentioned output unit An input means to input the digital content transmitted from the above-mentioned processor, The information processor characterized by having a decode processing means to perform decode processing using the cryptographic key information shared with the above-mentioned processor, and an output means to output the digital content after decoding an encryption part, to the inputted digital content.
[Claim 2] In the information processor equipped with the processor and the output unit at least the above-mentioned processor A cipher-processing means to perform cipher processing to a part of digital content using the cryptographic key information shared with the above-mentioned output unit, It has a transfer means to transmit the digital content as which the part was enciphered to the above-mentioned output unit. The above-mentioned output unit An input means to input the digital content transmitted from the above-mentioned processor, The information processor characterized by having a decode processing means to perform decode processing using the cryptographic key information shared with the above-mentioned processor, and an output means to output the digital content after decoding an encryption part, to the inputted digital content.
[Claim 3] In the information processor equipped with the processor and the output unit at least the above-mentioned processor As opposed to the digital content inputted as an input means to input the enciphered digital content A decode processing means to perform decode processing using the cryptographic key information for decoding this digital content, A cipher-processing means to perform cipher processing to a part of digital content after decode using the cryptographic key information shared with the above-mentioned output unit, It has a transfer means to transmit the enciphered digital content to the above-mentioned output unit. The above-mentioned output unit An input means to input the digital content transmitted from the above-mentioned processor, The information processor characterized by having a decode processing means to perform decode processing using the cryptographic key information shared with the above-mentioned processor, and an output means to output the digital content after decoding an encryption part, to the inputted digital content.
[Claim 4] The information processor characterized by to have an input means input the enciphered digital content, a decode processing means perform decode processing using the cryptographic key information for decoding this digital content to the digital content which inputted, a cipher-processing means perform cipher processing to a part of digital content after decode using the cryptographic key information which shares with the output unit of the output destination change of this digital content, and a transfer means transmit the digital content as which a part was enciphered to the above-mentioned output unit.
[Claim 5] It is the information processor which it is an information processor according to claim 3 or 4, and the digital content which the above-mentioned input means inputs makes one unit the formatting unit of the digital content at the time of a plaintext, and is characterized by being enciphered as some units of these units serve as a candidate for encryption.
[Claim 6] It is the information processor characterized by being an information processor according to claim 2, 3, 4, or 5, and for the above-mentioned cipher-processing means making one unit the formatting unit of the digital content at the time of a plaintext, and performing cipher processing for some units of these units as a processing object of cipher processing.
[Claim 7] It is the information processor which the above-mentioned cipher-processing means makes one unit voice data for two or more samples about the voice data outputted to the above-mentioned voice regenerative apparatus when it is an information processor according to claim 2, 3, 4, or 5 and the above-mentioned output

unit is a voice regenerative apparatus, and is characterized by performing cipher processing for some units of these units as a processing object of cipher processing.
[Claim 8] When it is an information processor according to claim 2, 3, 4, or 5 and the above-mentioned output unit is a display, the above-mentioned cipher-processing means In the direction of Rhine of the indicative data outputted to the above-mentioned indicating equipment, the indicative data for two or more lines is made into one unit. Some units of these units as a processing object of cipher processing The information processor which makes one unit the indicative data for two or more columns in the direction of a column of the indicative data which performs cipher processing or is outputted to the above-mentioned indicating equipment, and is characterized by performing cipher processing for some units of these units as a processing object of cipher processing.
[Claim 9] It is the information processor which the above-mentioned cipher-processing means makes one unit the data for 1 pixel of the indicative data outputted to the above-mentioned indicating equipment when it is an information processor according to claim 2, 3, 4, or 5 and the above-mentioned output unit is an indicating equipment, and is characterized by performing cipher processing for the part as a processing object of cipher processing respectively about a part or all of these units.
[Claim 10] The display characterized by having an input means to input the enciphered indicative data, a decode processing means to perform decode processing to the inputted indicative data using the cryptographic key information shared with the information processor of the source of this indicative data, and a display means to display the indicative data after decoding an encryption part.
[Claim 11] The digital content which is an indicating equipment according to claim 10, and the above-mentioned input means inputs [whether in the direction of Rhine of the indicative data at the time of a plaintext, as the indicative data for two or more lines is made into one unit and some units of these units serve as a processing object of cipher processing, it is enciphered, and] Or the display which makes one unit the indicative data for two or more columns in the direction of a column of the indicative data at the time of a plaintext, and is characterized by being enciphered as some units of these units serve as a processing object of cipher processing.
[Claim 12] It is the display which is an information processor according to claim 10, and the digital content which the above-mentioned input means inputs makes one unit the data for 1 pixel of the indicative data at the time of a plaintext, and is characterized by enciphering it respectively about a part or all of these units as the part serves as a processing object of cipher processing.
[Claim 13] In the digital content distribution system equipped with the digital content distribution equipment which distributes a digital content, and the information processor which transmits and outputs the digital content distributed from digital content distribution equipment to an output unit the above-mentioned digital content distribution equipment An are recording means by which the digital content as which the part was enciphered using the 1st cryptographic key information shared with the above-mentioned information processor is accumulated, It has a distribution means to distribute the accumulated digital content to the above-mentioned information processor. The above-mentioned information processor An input means to input the digital content distributed from the above-mentioned digital content distribution equipment, A decode processing means to perform decode processing to the encryption part in the inputted digital content using the cryptographic key information on the above 1st, A cipher-processing means to perform cipher processing to a part of digital content after decoding an encryption part using the 2nd cryptographic key information shared with the above-mentioned output unit, It has a transfer means to transmit the enciphered digital content to the above-mentioned output unit. The above-mentioned output unit An input means to input the digital content transmitted from the above-mentioned information processor, A decode processing means to perform decode processing to the encryption part in the inputted digital content using the cryptographic key information on the above 2nd, It has an output means to output the digital content after decoding an encryption part. The cipher-processing means of the above-mentioned digital content distribution equipment, and the cipher-processing means of the above-mentioned information processor The digital content distribution system which makes one unit the formatting unit of the digital content at the time of a plaintext, and is characterized by performing cipher processing for some units of these units as a processing object of cipher processing.
[Claim 14] In the digital content distribution system equipped with the digital content distribution equipment which distributes a digital content, and the information processor which transmits and outputs the digital content distributed from digital content distribution equipment to an output unit It is the approach of distributing a digital content to the above-mentioned information processor from the above-mentioned digital content distribution equipment, and outputting with the above-mentioned output unit. The above-mentioned digital content

distribution equipment the digital content as which the part was enciphered using the 1st cryptographic key information shared with the above-mentioned information processor As opposed to the encryption part in the digital content to which it distributes to the above-mentioned information processor, and the above-mentioned information processor is distributed from the above-mentioned digital content distribution equipment Perform decode processing using the cryptographic key information on the above 1st, and a part of digital content after decoding an encryption part is received. After performing cipher processing using the 2nd cryptographic key information shared with the above-mentioned output unit As opposed to the encryption part in the digital content to which the digital content after encryption is transmitted to the above-mentioned output unit, and the above-mentioned output unit is transmitted from the above-mentioned information processor Perform decode processing using the cryptographic key information on the above 2nd, and that of the digital content after decoding an encryption part is outputted. The digital content which the above-mentioned digital content distribution equipment distributes, and the digital content which the above-mentioned information processor transmits The digital content distribution and the output method which makes one unit the formatting unit of the digital content at the time of a plaintext, and is characterized by being enciphered as some units in these units serve as a candidate for encryption.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention distributes a digital content and relates to the approach of outputting with the information processor of a distribution place, enabling use in the form which stimulates audiovisual desire of the user who prevents the unauthorized use by the duplicate especially, and does not have a just use right about the technique of treating the digital content which needs protection of copyrights.
[0002]
[Description of the Prior Art] recent years, an image, voice, etc. -- high -- the demand which distributes added value information by the digital format is increasing, and in order to plan the protection of copyrights of a digital content, importance has been attached to prevention of an illegal copy. That is, since quality does not deteriorate even if it copies when it can copy easily, evils, such as infringement of the copyright by the illegal copy, are already producing a digital content.
[0003] Encryption of a digital content is used, and only the user who received just cryptographic key information decodes the enciphered digital content, and enables it to confirm the contents generally as one of the anti-copying means.
[0004]
[Problem(s) to be Solved by the Invention] If there is no just cryptographic key information, it will become impossible however, to completely view and listen to the enciphered digital content, when a digital content is enciphered simply.
[0005] This is because it becomes impossible for the software and hardware which the DS of a digital content will be destroyed and reproduce a digital content to completely interpret DS by performing simple encryption which disregarded the format, in spite of formatting the digital content according to a certain format.
[0006] Then, unless a user purchases a digital content and just cryptographic key information comes to hand, the contents will not be able to be confirmed but the threshold of digital content purchase will become high for a user.

[0007] Although right protection of a digital content is made into a major premise in order to solve such a problem, it is desirable to distribute a digital content in the form which stimulates audiovisual desire of a user.
[0008] Moreover, conventionally, encryption of a digital content is performed only about the path until it reaches a user's information processor, and is not set as the object of the protection of copyrights by encryption in the information processor about the path at the time of outputting to final output equipments, such as a display.
[0009] Since the final output equipment of a digital input like a liquid crystal display is becoming common in recent years instead of the final output equipment of an analog input like the conventional CRT (Cathode-Ray Tube) indicating equipment, there is a possibility that the illegal copy of a digital content may be performed, in the path at the time of outputting to such final output equipment.
[0010] Then, the purpose of this invention is in an information processor to make it possible to prevent the illegal copy in the path at the time of finally outputting a digital content.
[0011] Moreover, in an information processor, another purpose of this invention is by stimulating audiovisual desire of a user to make it possible to promote distribution or sale of contents at the time of digital one while protecting the right of a digital content.
[0012]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, this invention transmits the digital content which the above-mentioned processor enciphered using the cryptographic key information shared with the above-mentioned output unit in the information processor equipped with the processor and the output unit at least to the above-mentioned above-mentioned output unit, and the above-mentioned output unit is made to perform decode processing to the digital content transmitted from the above-mentioned processor using the above-mentioned cryptographic key information.
[0013] And especially, in order to attain another purpose, the digital content transmitted to the above-mentioned output unit from the above-mentioned processor makes one unit the formatting unit of the digital content at the time of a plaintext, and they are made to be enciphered in this invention, as some units of these units serve as a candidate for encryption.
[0014]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to a drawing.
[0015] Drawing 1 is the outline block diagram of the digital content distribution system concerning this operation gestalt.
[0016] For 100, as for an information processor and 102, digital content distribution equipment and 101 are [the body of an information processor and 103] displays among drawing.
[0017] The digital content distribution system concerning this operation gestalt makes the major premise right protection of the high added value contents distributed as digital data by digital content distribution equipment 100. That is, the digital content (distribution data) by which between digital content distribution equipment 100 and the bodies 102 of an information processor is transmitted to the digital content distribution system concerning this operation gestalt, and the digital content (indicative data) to which between the body 102 of an information processor and indicating equipments 103 is transmitted are aiming at protection by having enciphered these for what is digital data respectively.
[0018] And the digital content distribution system concerning this operation gestalt aims at enabling distribution of a digital content in the form which stimulates audiovisual desire of a user. That is, the digital content distribution system concerning this operation gestalt is the enciphered digital content, and makes it possible to stimulate an audiovisual demand of a user.
[0019] Specifically, the digital content to which between digital content distribution equipment 100 and the bodies 102 of an information processor is transmitted is encryption data enciphered with the cipher system with which the digital data formatted by compression methods decided beforehand, such as JPEG (Joint Photographic Experts Group) and MPEG (Moving Picture Experts Group), was decided [DES / (Data Encryption Standard)] beforehand.
[0020] Here, even if digital content distribution equipment 100 is network equipment which distributes a digital content via a network, it may be the record medium with which digital contents, such as an optical disk medium and a magnetic-disk medium, were recorded, for example.
[0021] That is, digital content distribution equipment 100 may not perform cipher processing that it should just be enciphered when the digital content distributed by digital content distribution equipment 100 is distributed from digital content distribution equipment 100.
[0022] Now, as shown in drawing 1 , it sets to the digital content distribution system concerning this operation

gestalt, and digital content distribution equipment 100 and the body 102 of an information processor have the function to share the cryptographic key information 104 for enciphering / decrypting a digital content (distribution data) by a certain approach.
[0023] About the approach of sharing the cryptographic key information 104, various approaches serve as a well-known technique, and what kind of approach may be adopted.
[0024] For example, the approach the body 102 of an information processor receives the cryptographic key information 104 is mentioned from the network equipment which has managed the cryptographic key information 104 used for encryption of a digital content. Network equipment enciphers the cryptographic key information 104 using the public key information on the body 102 of an information processor, and it is made for the body 102 of an information processor to decode for the private key information on own at this time.
[0025] Moreover, the method of recording the cryptographic key information 104 used for encryption of the digital content (finishing [encryption]) currently recorded on the magnetic-disk medium, for example on the nonvolatile storage inside the body 102 of an information processor at the time of manufacture of the body 102 of an information processor is mentioned.
[0026] Similarly, as shown in drawing 1 , it sets to the digital content distribution system concerning this operation gestalt, and the body 102 of an information processor and the indicating equipment 103 have the function to share the cryptographic key information 105 for enciphering / decrypting a digital content (indicative data) by a certain approach.
[0027] Also about the approach of sharing the cryptographic key information 105, like the approach of sharing the cryptographic key information 104, various approaches serve as a well-known technique, and what kind of approach may be adopted.
[0028] For example, the approach a display 103 receives the cryptographic key information 105 which the body 102 of an information processor used for encryption of a digital content from the body 102 of an information processor is mentioned. The body 102 of an information processor enciphers the cryptographic key information 105 using the public key information on a display 103, and it is made for a display 103 to decode for the private key information on own at this time.
[0029] Moreover, for example, the method of recording the cryptographic key information 105 on the nonvolatile storage of each interior at the time of manufacture of the body 102 of an information processor and a display 103 is mentioned.
[0030] Moreover, as shown in drawing 1 , it sets to the digital content distribution system concerning this operation gestalt. As opposed to the encryption part in the digital content to which the body 102 of an information processor is distributed from (1) digital-content distribution equipment 100 The decode function to perform decode processing 106 using the cryptographic key information 104, the expansion function to perform expansion processing 107 of the digital content after decoding (2) encryption parts, (3) As opposed to a part of the display-control function and (4) indicative datas which perform display-control processing 108 changed into the indicative data for outputting the developed digital content with the bit rate which an indicating equipment 103 requires It has the code function to perform cipher processing 109 using the cryptographic key information 105.
[0031] Moreover, as shown in drawing 1 , in the digital content distribution system concerning this operation gestalt, the display 103 has the decode function to perform decode processing 110 using the cryptographic key information 105, and the display function which performs display processing 111 of the indicative data after decoding (2) encryption parts to the encryption part in the indicative data enciphered by the code function of the body 102 of (1) information processor.
[0032] Next, outline actuation of the digital content distribution system concerning this operation gestalt is explained using drawing 2 .
[0033] Drawing 2 is the outline operation flow chart of the digital content distribution system concerning this operation gestalt.
[0034] Setting to drawing 2 , digital content distribution equipment 100 and the body 102 of an information processor first share the cryptographic key information 104 for enciphering / decrypting a digital content (distribution data) by a certain approach (step 201). Since various approaches serve as a well-known technique about the approach of sharing the cryptographic key information 104 and what kind of approach may be adopted as mentioned above, it does not specify here.
[0035] Then, digital content distribution equipment 100 distributes the digital content as which the part was enciphered using the cryptographic key information 104 to the body 102 of an information processor (step 202). As mentioned above, digital content distribution equipment 100 may not perform cipher processing that what is

necessary is to just be enciphered when the digital content distributed by digital content distribution equipment 100 is distributed from digital content distribution equipment 100.
[0036] Then, the body 102 of an information processor performs decode processing 106 using the cryptographic key information 104 to the encryption part in the digital content distributed from digital content distribution equipment 100 (step 203). By processing of step 203, the body 102 of an information processor will obtain the digital content of a plaintext to the interior.
[0037] Then, the body 102 of an information processor performs expansion processing 107 of the digital content obtained by processing of step 203 (step 204). For example, when the digital content obtained by processing of step 203 is MPEG data formatted by the MPEG method, the body 102 of an information processor will obtain the dynamic-image data which become the interior from per second 30 frames by processing of step 204.
[0038] Then, display-control processing 108 for outputting with the bit rate which an indicating equipment 103 requires to the indicative data containing the dynamic-image data obtained by processing of step 204 is performed (step 205). For example, when a display 103 is a TFT (Thin FilmTransistor) liquid crystal display, in processing of step 205, the body 102 of an information processor generates the sequential indicative data of about per second 60-70 frames.
[0039] Then, the body 102 of an information processor and an indicating equipment 103 share the cryptographic key information 105 for enciphering / decrypting a digital content (indicative data) by a certain approach (step 206). Since various approaches serve as a well-known technique about the approach of sharing the cryptographic key information 105 and what kind of approach may be adopted as mentioned above, it does not specify here.
[0040] Then, the body 102 of an information processor performs cipher processing 109 to the part in the indicative data generated by processing of step 205 using the cryptographic key information 105 (step 207). By processing of step 207, the body 102 of an information processor will obtain the indicative data as which the part was enciphered by the interior.
[0041] Then, the body 102 of an information processor outputs the indicative data as which the part was enciphered to an indicating equipment 103 (step 208).
[0042] Then, an indicating equipment 103 performs decode processing 110 using the cryptographic key information 105 to the encryption part in the indicative data outputted from the body 102 of an information processor (step 209). By processing of step 209, an indicating equipment 103 will obtain the indicative data of a plaintext to the interior.
[0043] Then, an indicating equipment 103 performs display processing 111 of the indicative data obtained by processing of step 209 (step 210). The indicative data which contains the dynamic-image data obtained by processing of step 204 by processing of step 210 will be displayed.
[0044] As mentioned above, the digital content distributed from digital content distribution equipment 100 will be displayed by processing of step 201 - step 210 with a display 103.
[0045] In addition, below, the actuation realized by processing of step 201 - step 204 among actuation of the digital content distribution system concerning this operation gestalt is called "distribution path encryption" actuation, and the actuation realized by processing of step 205 - step 210 is called "output path encryption" actuation.
[0046] Moreover, even if processing of step 206 is performed in advance of distribution path encryption actuation, it may be carried out in parallel. Moreover, depending on the configuration of an information processor 101, sequence may reverse processing of step 205, step 206, and step 207.
[0047] Next, the detail of distribution path encryption actuation is explained.
[0048] First, outline actuation of the information processor 101 concerning this operation gestalt is explained using drawing 3 .
[0049] Drawing 3 is the outline block diagram of the information processor 101 concerning this operation gestalt.

[0050] By drawing 3 , it is a part about a display among the information processors 101, such as a personal computer (PC), and only the part about distribution path encryption actuation is shown.
[0051] the inside of drawing, and 102 -- the body of an information processor, and 103 -- a display and 104 -- cryptographic key information and 301 -- a central processing unit (CPU:Central Processing Unit) and 302 -- a system memory and 303 -- for an input control unit and 306, as for a bus and 308, the CCE and 307 are [a display control and 304 / display memory and 305 / the decode processing section and 309] the contents expansion processing sections.
[0052] In drawing 3 , when digital content distribution equipment 100 is network equipment, CCE 306 inputs a

digital content according to directions of CPU301. Moreover, when digital content distribution equipment 100 is a record medium, an input control unit 305 inputs a digital content according to directions of CPU301. The digital content which CCE 306 or an input control unit 305 inputted is inputted into a display control 303 through a bus 307 according to directions of CPU301.

[0053] In a display control 303, the decode processing section 308 performs decode processing 106 to the encryption part in the inputted digital content using the cryptographic key information 104 currently held inside the display control 303, and obtains the digital content of a plaintext inside a display control 303. Then, the contents expansion processing section 309 performs expansion processing 107 of a digital content which the decode processing section 308 decoded, and obtains the digital content developed inside the display control 303

[0054] The actuation so far is equivalent to distribution path encryption actuation. About the detail of subsequent output path encryption actuation, it mentions later.

[0055] In addition, the decode processing section 308 and the contents expansion processing section 309 may be made to be mounted in a display control 303 as hardware, and prepare CPU and memory original in a display control 303, and may be made to be mounted as software.

[0056] Next, distribution path encryption actuation explains an example of the encryption approach of the digital content distributed from digital content distribution equipment 100 using drawing 5 and drawing 6 .

[0057] Drawing 5 is the explanatory view showing an example of the encryption approach of the digital content distributed from digital content distribution equipment 100, and drawing 6 is the explanatory view showing the display image at the time of displaying the digital content enciphered by the encryption approach shown in drawing 5 with an indicating equipment 103.

[0058] In drawing 5 and drawing 6 , the case where a digital content is MPEG data is made into the example.

[0059] An one-frame mxn pixel and the dynamic-image data which consist of per second k frames are classified into three formats, I picture format, P picture format, and B picture format, according to compression by the MPEG method, for example.

[0060] (1) In an I picture formal I picture format, after the image data of an one-frame mxn pixel is divided into two or more 8x8-pixel blocks, and orthogonal transformation processing is performed for every block and changed into frequency-domain data, it quantizes and a data compression is performed. In I picture data, coding only for the data in a former frame is made, and one frame data are obtained from I picture data by expansion processing.

[0061] (2) In a P picture formal P picture format, the data compression which performed inter-frame prediction of the forward direction is performed. P picture data -- difference with I picture -- coding using information is made and P picture data and I picture data used as former drawing are needed for restoration of a former frame. That is, image data is not obtained only with P picture data.

[0062] (3) In a B picture formal B picture format, the data compression which performed bidirectional inter-frame prediction is performed. B picture data -- the difference between I picture and P picture -- coding using information is made and P picture data, I picture data used as former drawing, and B picture data are needed for restoration of a former frame. That is, image data is not obtained only with B picture data.

[0063] Moreover, the sign allotment of one picture data becomes small in order of I picture, P picture, and B picture, as shown in drawing 5 . Dynamic-image data are encoded in sequence, such as IBB, PBB, PBB, IBB, PBB, and PBB, for every frame.

[0064] The following three approaches can be considered as the MPEG data encryption approach with such a property.

[0065] (1) As the encryption approach of the 1st encryption approach 1st, there is a method of enciphering only I picture data. The 1st encryption approach is further divided into the approach of enciphering for every high frequency field data / low frequency field data of /Not giving, paying attention to the frequency component within the approach of enciphering for every block used as a compression unit of /Not giving, and the block used as a compression unit.

[0066] First, if the former approach (the approach of enciphering for every block used as a compression unit of /not giving) is explained, in case encryption by this approach will be performed, for example to the former image shown in drawing 6 (a), a block is made into the processing object of cipher processing, cipher processing is performed to a certain block, and it is made not to perform cipher processing to a certain block.

[0067] If the MPEG data enciphered by this approach do not perform decode processing which used the cryptographic key information 104, the image at the time of being displayed on an indicating equipment 103 comes to be shown in drawing 6 (b). By this approach, by making the block count which enciphers fluctuate, it is

controllable in the dirt degree of a former image, and can change freely what indication is performed.
[0068] Next, if the latter approach (the approach of enciphering for every high frequency field data / low frequency field data of /not giving) is explained, in case encryption by this approach will be performed, for example to the former image shown in drawing 6 (a), the low frequency field data within a block are made into the processing object of cipher processing, cipher processing is performed to the low frequency field data under each block, and it is made not to perform cipher processing to high frequency field data. If the MPEG data enciphered by this approach do not perform decode processing which used the cryptographic key information 104, the image at the time of being displayed on an indicating equipment 103 comes to be shown in drawing 6 (c).

[0069] Although it will not illustrate if high frequency field data are enciphered, although it will become difficult for a former image to be polluted greatly and to observe a former image as shown in drawing 6 (c) if low frequency field data are enciphered, it becomes the image superimposed on the noise by the former image.
[0070] By this approach, by choosing the frequency domain which enciphers, it is controllable in the dirt degree of a former image, and can change freely what indication is performed. Moreover, even if it does not make all blocks into the processing object of cipher processing, it is good also considering a part of blocks as a processing object of cipher processing.
[0071] when only I picture data is enciphered by the 1st encryption approach, and there is no cryptographic key information 104, I picture data cannot be restored, therefore it is shown in drawing 5 -- as -- the difference of I picture data -- P picture data and B picture data which are information also become impossible [also developing these], although not enciphered. For example, when there are no dynamic-image data of 104 cryptographic key information encoded in order of IBB, PBB, PBB, IBB, PBB, and PBB, it becomes xxx, xxx, xxx, xxx, xxx, and xxx (x means failure in normal decode and expansion.), and a former image with all normal frames is not obtained.
[0072] (2) As the encryption approach of the 2nd encryption approach 2nd, there is a method of enciphering only P picture data. The 2nd encryption approach is also further divided into the approach of enciphering for every high frequency field data / low frequency field data of /Not giving, like the 1st encryption approach paying attention to the frequency component within the approach of enciphering for every block used as a compression unit of /Not giving, and the block used as a compression unit.
[0073] when only P picture data is enciphered by the 2nd encryption approach, and there is no cryptographic key information 104, P picture data cannot be restored, therefore it is shown in drawing 5 -- as -- the difference of I picture data and P picture data -- B picture data which is information also becomes impossible [also developing this], although not enciphered. For example, the dynamic-image data of 104 cryptographic key information encoded in order of IBB, PBB, PBB, IBB, PBB, and PBB become Ixx, xxx, xxx, Ixx, xxx, and xxx (x means failure in normal decode and expansion.), when there is nothing, and the normal image frame obtained serves as only I picture data.
[0074] (3) As the encryption approach of the 3rd encryption approach 3rd, there is a method of enciphering only B picture data. The 3rd encryption approach is also further divided into the approach of enciphering for every high frequency field data / low frequency field data of /Not giving, like the 1st encryption approach paying attention to the frequency component within the approach of enciphering for every block used as a compression unit of /Not giving, and the block used as a compression unit.
[0075] When only B picture data is enciphered by the 3rd encryption approach, if there is no cryptographic key information 104 as shown in drawing 5 , B picture data cannot be restored. For example, the dynamic-image data of 104 cryptographic key information encoded in order of IBB, PBB, PBB, IBB, PBB, and PBB become Ixx, Pxx, Pxx, Ixx, Pxx, and Pxx (X means failure in normal decode and expansion.), when there is nothing, and the normal image frame obtained serves as only I picture data and P picture.
[0076] As mentioned above, although three approaches were explained as the MPEG data encryption approach, you may make it combine these approaches with arbitration.
[0077] Since a digital content is not enciphered simply, but the data made into the processing object of cipher processing are chosen in distribution path encryption actuation and he is trying to encipher only a part according to the digital content distribution system concerning this operation gestalt, when it does not have the just cryptographic key information 104, it will be in the condition that some former images were stained. Since it becomes possible since the value is spoiled to prevent the illegal copy of a digital content and a part of digital content is indicated, the digital content with which the part was soiled stimulates a viewing-and-listening demand of a user, and becomes possible [urging perfect viewing and listening of a digital content].
[0078] In case the data made into the processing object of cipher processing are chosen, he is trying to pay his

attention to the format in the digital content distribution system especially applied to this operation gestalt. Namely, although it will be completely impossible for all the DS called the header, the payload, and footer to be lost, and to use as a digital content when it considers as the processing object of cipher processing by making a digital content into a mere bit string In the digital content distribution system concerning this operation gestalt Since he is trying to choose the data which do not treat a digital content as a mere bit string, but are made into the processing object of cipher processing according to the significant taste part of a format, not the whole data but a part of dirt is possible.

[0079] Moreover, since cipher processing which used the cryptographic key information 104 for data dirt is used in distribution path encryption actuation, in order to stimulate viewing-and-listening desire of a user according to the digital content distribution system concerning this operation gestalt, it is not necessary to prepare a dirt digital content apart from a perfect digital content, and becomes that it is possible to reduce the cost concerning distribution and are recording of a digital content.

[0080] Furthermore, according to the digital content distribution system concerning this operation gestalt, in distribution path encryption actuation, mitigation of the throughput of cipher processing / decode processing is also possible by making a part of digital content into the processing object of cipher processing, and avoiding cipher processing to the whole digital content. In addition, whenever [dirt], and throughput have the relation of a trade-off, and modification of a priority is easily possible according to a demand.

[0081] It becomes possible to stimulate viewing-and-listening desire of a user, protecting copyright on the distribution path of a digital content by distribution path encryption actuation according to the digital content distribution system concerning this operation gestalt, as explained above.

[0082] In addition, the information processor 101 concerning this operation gestalt is made the configuration shown in drawing 7 instead of the configuration shown in drawing 3 , and software may be made to realize the decode processing section 308 and the contents expansion processing section 309 which were shown in drawing 3 .

[0083] Drawing 7 is other outline block diagrams of the information processor 101 concerning this operation gestalt.

[0084] Like [drawing 7] drawing 3 , it is a part about a display among the information processors 101, such as PC, and only the part about distribution path encryption actuation is shown.

[0085] The same sign is given among drawing to the same component as drawing 3 . 701 is a nonvolatile storage.

[0086] In the information processor 101 of a configuration of being shown in drawing 7 , CPU301 realizes actuation of the decode processing section 308 shown in drawing 3 , and the contents expansion processing section 309 by loading a program and performing on a system memory 302.

[0087] In drawing 7 , when digital content distribution equipment 100 is network equipment, CCE 306 inputs a digital content according to directions of CPU301. Moreover, when digital content distribution equipment 100 is a record medium, an input control unit 305 inputs a digital content according to directions of CPU301. The digital content which CCE 306 or an input control unit 305 inputted is inputted into a system memory 302 through a bus 307 according to directions of CPU301.

[0088] To the encryption part in the inputted digital content, CPU301 performs decode processing 106 using the cryptographic key information 104, and obtains the digital content of a plaintext on a system memory 302. Then, CPU301 performs decoded expansion processing 107 of a digital content, and obtains the developed digital content. The obtained digital content is inputted into a display control 303.

[0089] Here, by explanation which used drawing 3 , although held inside a display control 303, in the information processor 101 of a configuration of being shown in drawing 7 , as for the cryptographic key information 104, CPU301 shall also realize sharing of the cryptographic key information 104 by loading and performing a program on a system memory 302.

[0090] Moreover, also in any of drawing 3 and drawing 7 , although the information processor 101 concerning this operation gestalt is considered as the configuration equipped with information-processor 102 body and the display 103, it may be the configuration which the body 102 of an information processor and the display 103 unified. That is, it is good also as a Personal Digital Assistant called the so-called PDA (PersonalDigital Assistant) etc. in the information processor 101 concerning this operation gestalt.

[0091] Generally, since a Personal Digital Assistant is constituted using CPU with the comparatively low engine performance, the memory of small capacity, etc. in many cases, cipher processing which is comparatively heavy processing has the problem of becoming a big burden for a Personal Digital Assistant.

[0092] Then, if a Personal Digital Assistant with such a problem is used by the digital content distribution

system concerning this operation gestalt, when coexistence of the audiovisual desire stimulus of protection of copyrights and a user which this invention makes the purpose by treating the digital content as which not the whole but the part was enciphered is realizable, the load fall effectiveness by reduction of code throughput can be acquired. When a Personal Digital Assistant realizes cipher processing by software especially, it becomes unnecessary to carry highly efficient CPU and a highly efficient bulk memory in cipher processing, and effectiveness, such as low-cost-izing and low-power-izing, is acquired. Moreover, since processing speed required for the hardware only for cipher processing falls when a Personal Digital Assistant is equipped with the hardware only for cipher processing, effectiveness, such as low-power-izing by the low working speed and low-cost-izing by small-scale-izing of hardware logic, is acquired.

[0093] By the way, in above-mentioned explanation, although MPEG data (dynamic-image data) were made into the example, it is not necessarily aimed only at dynamic-image data.

[0094] For example, when a digital content is JPEG data (static-image data), it is possible to use the encryption approach of I picture data mentioned above and the same encryption approach.

[0095] Moreover, what is necessary is to perform band division to speech information, to be made to perform encryption only to the encryption/high frequency component only to a low-frequency component, or just to carry out as [encipher / every number sample], for example, since divided coding which became independent for every frequency component is performed when a digital content is MPEG data (voice data). Thus, if whenever [data dirt] is controlled, it will become possible to generate a jarring playback sound moderately.

[0096] Now, the detail of output path encryption actuation is explained below.

[0097] First, outline actuation of the information processor 101 concerning this operation gestalt is explained using drawing 4 .

[0098] Drawing 4 is the outline block diagram of the information processor 101 concerning this operation gestalt.

[0099] By drawing 4 , it is a part about a display among the information processors 101, such as PC, and only the part about output path encryption actuation is shown.

[0100] The same sign is given among drawing to the same component as drawing 3 . As for the cipher-processing section and 402, 401 is [the decode processing section and 403] data drivers.

[0101] Here, let displays 103 be for example, liquid crystal display (LCD:Liquid Crystal Display) equipment and a display of a digital input like the CRT (Cathode-RayTube) equipment possessing a digital to analog function.

[0102] In drawing 4 , the indicative data (plaintext indicative data) containing the digital content developed inside the display control 303 is accumulated in display memory 304 by the distribution path encryption actuation mentioned above according to directions of CPU301.

[0103] In a display control 303, the plaintext indicative data accumulated in display memory 304 is inputted, and the cipher-processing section 401 performs cipher processing 109 to a part of inputted plaintext indicative data using the cryptographic key information 105 currently held inside the display control 303, and obtains the indicative data enciphered inside the display control 303. The obtained encryption indicative data is inputted into a display 103 from a display control 303.

[0104] Then, in an indicating equipment 103, the decode processing section 402 performs decode processing 110 to the encryption part in the inputted encryption indicative data using the cryptographic key information 105 currently held inside the indicating equipment 103, and obtains a plaintext indicative data inside an indicating equipment 103. Then, the data driver 403 performs display processing 111 of a plaintext indicative data by supplying the plaintext indicative data which the decode processing section 402 decoded to each display pixel on a display screen.

[0105] The above actuation is equivalent to output path encryption actuation.

[0106] In addition, the cipher-processing section 402 may be made to be mounted in a display control 303 as hardware, and prepares CPU and memory original in a display control 303, and may be made to be mounted as software.

[0107] Next, outline actuation of the display control 303 concerning this operation gestalt is explained using drawing 8 .

[0108] Drawing 8 is the outline block diagram of the display control 303 concerning this operation gestalt.

[0109] Drawing 8 shows only the part about output path encryption actuation among display controls 303.

[0110] 801 among drawing the timing generation section and 803 for a memory control section and 802 A timing signal, 804 a memory address signal and 304 for a memory control signal and 805 Display memory, 806 a LCD control signal and 808 for a LCD control section and 807 A plaintext indicative data, 809 a LCD indicative data and 811 for a timing control section and 810 A serial/parallel-conversion circuit (S/P circuit), For an encryption

S/P finishing LCD indicative data and 814, as for an encryption LCD indicative data and 816, a parallel/serial-conversion circuit (P/S circuit) and 815 are [812 / a S/P finishing LCD indicative data and 813 / a delay circuit and 817] delayed LCD control signals.

[0111] In drawing 8 , using the timing signal 803 sent from the timing generation section 802, the memory control section 801 generates the memory control signal 804 and the memory address signal 805, and reads the plaintext indicative data 808 from display memory 304 one by one.

[0112] On the other hand, the LCD control section 806 generates the LCD control signal 807 which controls the display timing of LCD using the timing signal 803 sent from the timing generation section 802.

[0113] The timing control section 809 sends out the plaintext indicative data 809 read from display memory 304 as a LCD indicative data 810 according to the display timing by the LCD control signal 807.

[0114] That is, the plaintext indicative data 808 read from display memory 304 turns into the LCD indicative data 810 which synchronized with the LCD control signal 807 by the timing control section 809.

[0115] For example, supposing the LCD control signal 807 transmits the indicative data for 1 pixel by 1 data-transfer clock synchronization and consists of data whose 1 pixel is 16 bits, the LCD indicative data 810 will serve as a 16-bit data bus. Here, when a block cipher like DES is used for cipher processing, the cipher-processing section 401 will perform block cipher processing of 64 bitwises using the cryptographic key information 105.

[0116] In order to absorb the difference in both batch, in the display control 303 concerning this operation gestalt, the S/P circuit 812 and the P/S circuit 814 are used. The S/P circuit 811 is the data width of face (here) of the LCD indicative data 810. About 16 bitwises, it is a code batch (here). It is what changes into 64 bitwise width of face, and is supplied to the cipher-processing section 401 as a S/P finishing LCD indicative data 812. Moreover, the P/S circuit 814 The data width of face of the encryption S/P finishing LCD indicative data 813 after cipher processing was performed by the cipher-processing section 401 is changed into the data width of face of the LCD indicative data 810, and is supplied to the data driver 403 as an encryption LCD indicative data 815.

[0117] According to the data width of face of the LCD indicative data 810, and the code batch width of face of the cipher-processing section 401, the configurations of the S/P circuit 811 and the P/S circuit 814 differ.

[0118] In the display control 303 applied to this operation gestalt as shown in drawing 8 Since processing by the S/P circuit 811, the cipher-processing section 401, and the P/S circuit 814 is prepared By making it output delay equivalent to delay by these processings as a delayed LCD control signal 817 by the delay circuit 816 in addition to the LCD control signal 807 which the LCD control section 806 generated The encryption LCD indicative data 816 outputted is made to be supplied to the data driver 403 from the P/S circuit 814 synchronizing with the delayed LCD control signal 817.

[0119] Thereby, creation of the encryption LCD indicative data 815 based on performing cipher processing to a part of indicative data on the way of [of the display timing control by the display control 303 / processing], i.e., real-time cipher processing of the LCD indicative data 810, is attained.

[0120] Next, outline actuation of the display 103 concerning this operation gestalt is explained using drawing 9 .

[0121] Drawing 9 is the outline block diagram of the display 103 concerning this operation gestalt.

[0122] By drawing 9 , the case where a display 103 is a liquid crystal display is made into the example, and only the part (namely, liquid crystal drive drain side driver equivalent to the data driver 403) about output path encryption actuation is shown among displays 103.

[0123] A latch circuit -3,912 is a liquid crystal drive circuit where 901 generate the timing signal (CL1 signal) with which the incorporation signal (CL2 signal) of an encryption indicative data and 902 output an encryption indicative data, and 903 outputs LCD driver voltage, and the voltage level for [904] a liquid crystal drive in the power source for a LCD drive, the level shifter to which a latch circuit -2,909 carries out a liquid crystal drive output signal and 906 to a latch address selector, and 907 carries out the pressure up of the latch circuit -1,908 for 905 from circuit driver voltage to liquid crystal driver voltage and 910 among drawing, 911 is a plaintext indicative data

[0124] In drawing 9 , the latch address selector 906 is counting falling of CL2 signal 901 (it is equivalent to the delayed LCD control signal 817 shown in drawing 8 .) inputted from the display control 303 synchronizing with the input of the encryption indicative data 902, and generates the latch signal over a latch circuit -1 (907).

[0125] The encryption indicative data 902 inputted from the display control 303 is held on the latch circuit -1 (907) at entry sequence by the latch signal which the latch address selector 906 generates.

[0126] CL1 signal 903 is a Horizontal Synchronizing signal inputted for every display of one line, and the encryption indicative data 902 for 1 display Rhine latched by the input of CL1 signal 903 on the latch circuit -1

(907) is latched on every one-line latch circuit -2 (908) for every one-line display period.
[0127] Decode processing 100 which used the cryptographic key information 105 is performed by the decode processing section 402, and the encryption indicative data 902 for one line latched on the latch circuit -2 (908) turns into the plaintext indicative data 912, and is latched on every one-line latch circuit -3 (911) for every one-line display period by CL1 signal 903.
[0128] The plaintext indicative data 912 for one line latched on the latch circuit -3 (911) is changed into liquid crystal driver voltage through a level shifter 909 and the liquid crystal drive circuit 910, and is impressed to an one-line display period and liquid crystal.
[0129] By the above processing, the display action to liquid crystal is performed for every line.
[0130] When a block cipher like DES is used for decode processing, only the part in which parallel processing is possible makes coincidence arrange in parallel the number of bits to which the decode processing section 402 is outputted from a latch circuit -2 (908) per block here. For example, since a liquid crystal drive drain side driver will become 18432 bits per line supposing it is a 18-bit output per pixel with the 1024-pixel configuration per line, 288 blocks of 64 bitwises (batch by DES) are made to arrange in parallel. And the decode processing section 402 will perform block decode processing of 64 bitwises using the cryptographic key information 105.
[0131] Thereby, creation and a display of the plaintext indicative data 912 based on performing decode processing to a part of indicative data on the way of [of the display control by the liquid crystal drive drain side driver of an indicating equipment 103 / processing], i.e., real-time decode processing of the encryption indicative data 912, are attained.
[0132] In addition, the display 103 concerning this operation gestalt may be made the configuration shown in drawing 10 instead of the configuration shown in drawing 9 .
[0133] Drawing 10 is other outline block diagrams of the display 103 concerning this operation gestalt.
[0134] Drawing 10 as well as drawing 9 makes the example the case where a display 103 is a liquid crystal display, and only the part (namely, liquid crystal drive drain side driver equivalent to the data driver 403) about output path encryption actuation is shown among displays 103.
[0135] The same sign is given among drawing to the same component as drawing 9 . For 1001, as for a P/S circuit and 1003, a S/P circuit and 1002 are [a S/P finishing indicative data and 1004] plaintext indicative datas.
[0136] The indicating equipment 103 shown in drawing 10 the data width of face of the encryption indicative data 902 When it differs from the data width of face of the decode batch of the decode processing section 402 depending on the number of data bits and data transfer clock (CL2 signal 901) per pixel, by the S/P circuit 1001 After changing the data width of face of the encryption indicative data 902 into the data width of face of a suitable decode batch and considering as the S/P finishing indicative data 1003, by the decode processing section 402 Decode processing is performed using the cryptographic key information 105, and the plaintext indicative data 1004 obtained by decode processing is changed into the data width of face of the plaintext indicative data 912 by the P/S circuit 1002.
[0137] You may make it the decode processing section 402 make a processing block arrange in parallel according to the number of bits of the encryption indicative data 902 per pixel, and CL2 signal 901 that what is necessary is just to be able to process at least 1 block.
[0138] As mentioned above, although the case where a display 103 was a liquid crystal display was taken for the example and output path encryption actuation was explained, if it is made to perform same decode processing on the way which performs digital processing even when a display 103 is CRT equipment which possesses the digital to analog section by the digital input, creation and a display of a plaintext indicative data will be attained.
[0139] Next, output path encryption actuation explains an example of the encryption approach of the indicative data outputted from a display control 303 using drawing 11 and drawing 12 .
[0140] Drawing 11 is the explanatory view showing an example of the encryption approach of the indicative data outputted from a display control 303, and is the explanatory view showing the display image at the time of displaying the enciphered indicative data with an indicating equipment 103.
[0141] Drawing 11 shows the encryption approach of performing cipher processing in the direction of Rhine, and the encryption approach of performing cipher processing in the direction of a column, as the encryption approach of a former image (original plaintext indicative data).
[0142] (1) In case encryption by this approach is performed to the encryption approach (original plaintext indicative data), for example, the former image shown in drawing 11 (a), of performing cipher processing in the direction of Rhine, in the direction of Rhine, the indicative data for two or more lines (for example, about several lines) is made into one unit, and be made to perform cipher processing for some units of these units as a

processing object of cipher processing. It is made to repeat the case where the case where cipher processing is performed, and cipher processing are not specifically performed by turns for every indicative data for several lines.

[0143] If the indicative data enciphered by this approach performs decode processing which used the cryptographic key information 105, the image at the time of being displayed on an indicating equipment 103 will turn into the same image as the former image shown in drawing 11 (a), but if decode processing using the cryptographic key information 105 is not performed, the image at the time of being displayed on an indicating equipment 103 serves as the indicative data with which several lines were soiled at intervals of several lines, as shown in drawing 11 (b).

[0144] The number of Rhine made into one unit is determined beforehand, and while the cipher-processing section 401 of a display control 303 enciphers alternatively for every number of determined Rhine, it is made for the decode processing section 402 of a display 103 to decode alternatively by this approach. The dirt to a part of indicative data is attained by this, and it becomes reducible [the code / decode throughput in the cipher-processing section 401 of a display control 303, and the decode processing section 402 of a display 103].

[0145] Moreover, by making the number of Rhine made into one unit fluctuate, it is controllable in the dirt degree of an indicative data, and can change freely what indication is performed.

[0146] (2) In case encryption by this approach is performed to the encryption approach (original plaintext indicative data), for example, the former image shown in drawing 11 (a), of performing cipher processing in the direction of a column, in the direction of a column, the indicative data for two or more columns (for example, number column extent) is made into one unit, and be made to perform cipher processing for some units of these units as a processing object of cipher processing. It is made to repeat the case where the case where cipher processing is performed, and cipher processing are not specifically performed by turns for every indicative data for a number column.

[0147] If the indicative data enciphered by this approach performs decode processing which used the cryptographic key information 105, the image at the time of being displayed on an indicating equipment 103 will turn into the same image as the former image shown in drawing 11 (a), but if decode processing using the cryptographic key information 105 does not perform, the image at the time of being displayed on an indicating equipment 103 serves as the indicative data with which a part for a number column was soiled every number column, as shown in drawing 11 (c).

[0148] The number of columns made into one unit is determined beforehand, and while the cipher-processing section 401 of a display control 303 enciphers alternatively for every number of the determined columns, it is made for the decode processing section 402 of a display 103 to decode alternatively by this approach. The dirt to a part of indicative data is attained by this, and it becomes reducible [the code / decode throughput in the cipher-processing section 401 of a display control 303, and the decode processing section 402 of a display 103].

[0149] Moreover, by making the number of columns made into one unit fluctuate, it is controllable in the dirt degree of an indicative data, and can change freely what indication is performed.

[0150] Drawing 12 is the explanatory view showing an example of the encryption approach of the indicative data outputted from a display control 303, and shows the encryption approach of performing cipher processing to the part about the indicative data for 1 pixel in a former image (original plaintext indicative data), by drawing 12 .

[0151] By this approach, it is made to perform cipher processing only to the high order bit in the indicative data in 1 pixel, or made to perform cipher processing only to the lower bit in the indicative data in 1 pixel.

[0152] Only a high order bit is enciphered, and when a lower bit is considered as as [plaintext], the variation of an indicative data becomes large. Then, if it displays on an indicating equipment 103, without decoding an encryption indicative data, whenever [dirt / of data] will be large and observation of an indicative data will become difficult.

[0153] Moreover, when only a lower bit is enciphered and a high order bit considers as as [plaintext], there is little variation of an indicative data. Then, although whenever [dirt / of data] will be small and will be observed as a flicker on a screen if it displays on an indicating equipment 103, without decoding an encryption indicative data, rough observation of an indicative data is possible.

[0154] By drawing 12 , the indicative data for 1 pixel consisted of 8 bits, and when a certain plaintext indicative data was "55h", the example from which only the high order bit was enciphered, "55h" turned into "e5h", only the lower bit was enciphered, and "55h" turned into "52h" was shown. Thus, since the variation from a plaintext indicative data becomes large, the direction which enciphers only a high order bit will be observed as a more different display.

[0155] By this approach, it becomes it can be possible to choose the dirt degree of an indicative data, and reducible [the code / decode throughput in the cipher-processing section 401 of a display control 303, and the decode processing section 402 of a display 103] by choosing whether only a high order bit is enciphered or only a lower bit is enciphered.
[0156] As mentioned above, although the encryption approach of performing cipher processing in the direction of Rhine / the direction of a column, and the encryption approach of performing cipher processing only to the high order bit/lower bit in the indicative data in 1 pixel were explained, you may make it combine these approaches with arbitration.
[0157] According to the digital content distribution system concerning this operation gestalt, the protection of copyrights of the digital content in the output path to the indicating equipment 103 which is final output equipment which was not performed becomes possible conventionally by output path encryption actuation.
[0158] And since a digital content (indicative data) is not enciphered simply, but the data made into the processing object of cipher processing are chosen in output path encryption actuation and he is trying to encipher only a part according to the digital content distribution system concerning this operation gestalt, when it does not have the just cryptographic key information 105, it will be in the condition that some former images were stained. Since it becomes possible since the value is spoiled to prevent the illegal copy of a digital content and a part of digital content is indicated, the digital content with which the part was soiled stimulates a viewing-and-listening demand of a user, and becomes possible [urging perfect viewing and listening of a digital content].

[0159] Furthermore, according to the digital content distribution system concerning this operation gestalt, in output path encryption actuation, mitigation of the throughput of cipher processing / decode processing is also possible by making a part of digital content into the processing object of cipher processing, and avoiding cipher processing to the whole digital content. In addition, whenever [dirt], and throughput have the relation of a trade-off, and modification of a priority is easily possible according to a demand.
[0160] It becomes possible to stimulate viewing-and-listening desire of a user, protecting copyright on the output path of a digital content by output path encryption actuation according to the digital content distribution system concerning this operation gestalt, as explained above.
[0161] In addition, the information processor 101 concerning this operation gestalt is made the configuration shown in drawing 13 instead of the configuration shown in drawing 4 , and software may be made to realize the cipher-processing section 401 shown in drawing 4 .
[0162] Drawing 13 is other outline block diagrams of the information processor 101 concerning this operation gestalt.
[0163] Like [drawing 13] drawing 4 , it is a part about a display among the information processors 101, such as PC, and only the part about output path encryption actuation is shown.
[0164] The same sign is given among drawing to the same component as drawing 4 . 701 is a nonvolatile storage.

[0165] In the information processor 101 of a configuration of being shown in drawing 13 , CPU301 realizes actuation of the cipher-processing section 401 shown in drawing 4 by loading a program and performing on a system memory 302. That is, he is trying, as for the information processor 101 of a configuration of being shown in drawing 13 , for not the display control 303 but CPU301 to encipher an indicative data.
[0166] Drawing 14 is the explanatory view showing outline actuation of the information processor 101 of a configuration of being shown in drawing 13 .
[0167] As shown in drawing 14 , the plaintext indicative data 808 accumulated in display memory 304 is inputted into a system memory 302 through a display control 303 and a bus 307 according to directions of CPU301.
[0168] CPU301 performs cipher processing 109 to the inputted plaintext indicative data 808 using the cryptographic key information 105. the encryption indicative data 902 enciphered by CPU301 is boiled and inputted into display memory 304 through a bus 307 and a display control 303. The encryption indicative data 902 accumulated in display memory 304 is read by the display control 303, and is outputted to a display 103.
[0169] That is, in the information processor 101 of a configuration of being shown in drawing 13 , CPU301 generates the plaintext indicative data 808 on display memory 304, and generates the encryption indicative data 902 on display memory 304 from the plaintext indicative data 808 further. A display control 303 performs read-out actuation of the encryption indicative data 902, and performs a display action.
[0170] Here, although the cryptographic key information 105 shall be held inside a display control 303 by the explanation which used drawing 4 , in the information processor 101 of a configuration of being shown in drawing 13 , the cryptographic key information 105 shall be held at the nonvolatile storage 701.

[0171] Moreover, in any of drawing 4 and drawing 13 , although the information processor 101 concerning this operation gestalt is considered as the configuration equipped with information-processor 102 body and the display 103, as distribution path encryption actuation explained, it may be the configuration which the body 102 of an information processor and the display 103 unified. That is, it is good also as a Personal Digital Assistant called the so-called PDA etc. in the information processor 101 concerning this operation gestalt.
[0172] Since a Personal Digital Assistant is generally constituted using CPU with the comparatively low engine performance, the memory of small capacity, etc. in many cases as mentioned above, cipher processing which is comparatively heavy processing has the problem of becoming a big burden for a Personal Digital Assistant.
[0173] Then, if a Personal Digital Assistant with such a problem is used by the digital content distribution system concerning this operation gestalt, when coexistence of the audiovisual desire stimulus of protection of copyrights and a user which this invention makes the purpose by treating the digital content as which not the whole but the part was enciphered is realizable, the load fall effectiveness by reduction of code throughput can be acquired. When a Personal Digital Assistant realizes cipher processing by software especially, it becomes unnecessary to carry highly efficient CPU and a highly efficient bulk memory in cipher processing, and effectiveness, such as low-cost-izing and low-power-izing, is acquired. Moreover, since processing speed required for the hardware only for cipher processing falls when a Personal Digital Assistant is equipped with the hardware only for cipher processing, effectiveness, such as low-power-izing by the low working speed and low-cost-izing by small-scale-izing of hardware logic, is acquired.
[0174] By the way, in above-mentioned explanation, although the output to a digital display unit was made into the example, it is not necessarily aimed only at the display.
[0175] For example, also in an audio output device with a digital input, it is possible to realize output unit path encryption actuation by enciphering every number sample similarly to the voice data by which PCM (Pulse CodeModulation) coding was carried out.
[0176] When it does not have just cryptographic key information because it is made to perform cipher processing in the form depending on a format of a digital content to a part of digital content, he is trying for the digital content distribution system concerning this operation gestalt to serve as a digital content with which the part was soiled, as explained above. Then, it becomes possible to stimulate audiovisual desire of a user, protecting the copyright of a digital content.
[0177] Therefore, according to the digital content distribution system concerning this operation gestalt, it becomes possible to circulate the high digital content of added value on a semi-conductor storage or a digital network safely, and becomes applicable to digital content distribution service etc.
[0178] In addition, in protection of a digital content, it is good also as a system using either distribution path encryption actuation or the output path encryption actuation, and good also as a system which combines both and protects a digital content with two independent cipher systems.
[0179]
[Effect of the Invention] The final output of a digital content which can stimulate audiovisual desire of a user becomes possible, protecting the copyright of a digital content according to this invention, as explained above.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The outline block diagram of the digital content distribution system concerning this operation gestalt.

[Drawing 2] The outline operation flow chart of the digital content distribution system concerning this operation gestalt.
[Drawing 3] The outline block diagram of the information processor concerning this operation gestalt.
[Drawing 4] The outline block diagram of the information processor concerning this operation gestalt.
[Drawing 5] The explanatory view showing an example of the encryption approach of the digital content distributed from digital content distribution equipment.
[Drawing 6] The explanatory view showing the display image at the time of displaying the digital content enciphered by the encryption approach shown in drawing 5 with an indicating equipment.
[Drawing 7] The outline block diagram of the information processor concerning this operation gestalt.
[Drawing 8] The outline block diagram of the display control concerning this operation gestalt.
[Drawing 9] The outline block diagram of the display concerning this operation gestalt.
[Drawing 10] The outline block diagram of the display concerning this operation gestalt.
[Drawing 11] The explanatory view showing an example of the encryption approach of the indicative data outputted from a display control.
[Drawing 12] The explanatory view showing an example of the encryption approach of the indicative data outputted from a display control.
[Drawing 13] The outline block diagram of the information processor concerning this operation gestalt.
[Drawing 14] The explanatory view showing outline actuation of the information processor shown in drawing 13 .
[Description of Notations]
100: Digital content distribution equipment
101: Information processor
102: The body of an information processor
103: Display
104: Cryptographic key information
105: Cryptographic key information
106: Decode processing
107: Contents expansion processing
108: Display-control processing
109: Cipher processing
110: Decode processing
111: Display processing
301: Central processing unit (CPU:Central Processing Unit)
302: System memory
303: Display control
304: Display memory
305: Input control unit
306: Communication controller
307: Bus
308: Decode processing section
309: Contents expansion processing section
401: Cipher-processing section
402: Decode processing section
403: Data driver
701: Nonvolatile storage
801: Memory control section
802: Timing generation section
803: Timing signal
804: Memory control signal
805: Memory address signal
806: LCD (Liquid Crystal Display) control section
807: LCD control signal
808: Plaintext indicative data
809: Timing control section
810: LCD indicative data
811: Serial/parallel-conversion circuit (S/P circuit)

812: S/P finishing LCD indicative data
813: Encryption S/P finishing LCD indicative data
814: Parallel/serial-conversion circuit (P/S circuit)
815: Encryption LCD indicative data
816: Delay circuit
817: Delayed LCD control signal
901: CL2 signal
902: Encryption indicative data
903: CL1 signal
904: The power source for a LCD drive
905: Liquid crystal drive output signal
906: Latch address selector
907: Latch circuit -1
908: Latch circuit -2
909: Level shifter
910: Liquid crystal drive circuit
911: Latch circuit -3
912: Plaintext indicative data
1001: S/P circuit
1002: P/S circuit
1003: S/P finishing indicative data
1004: Plaintext indicative data

[Translation done.]

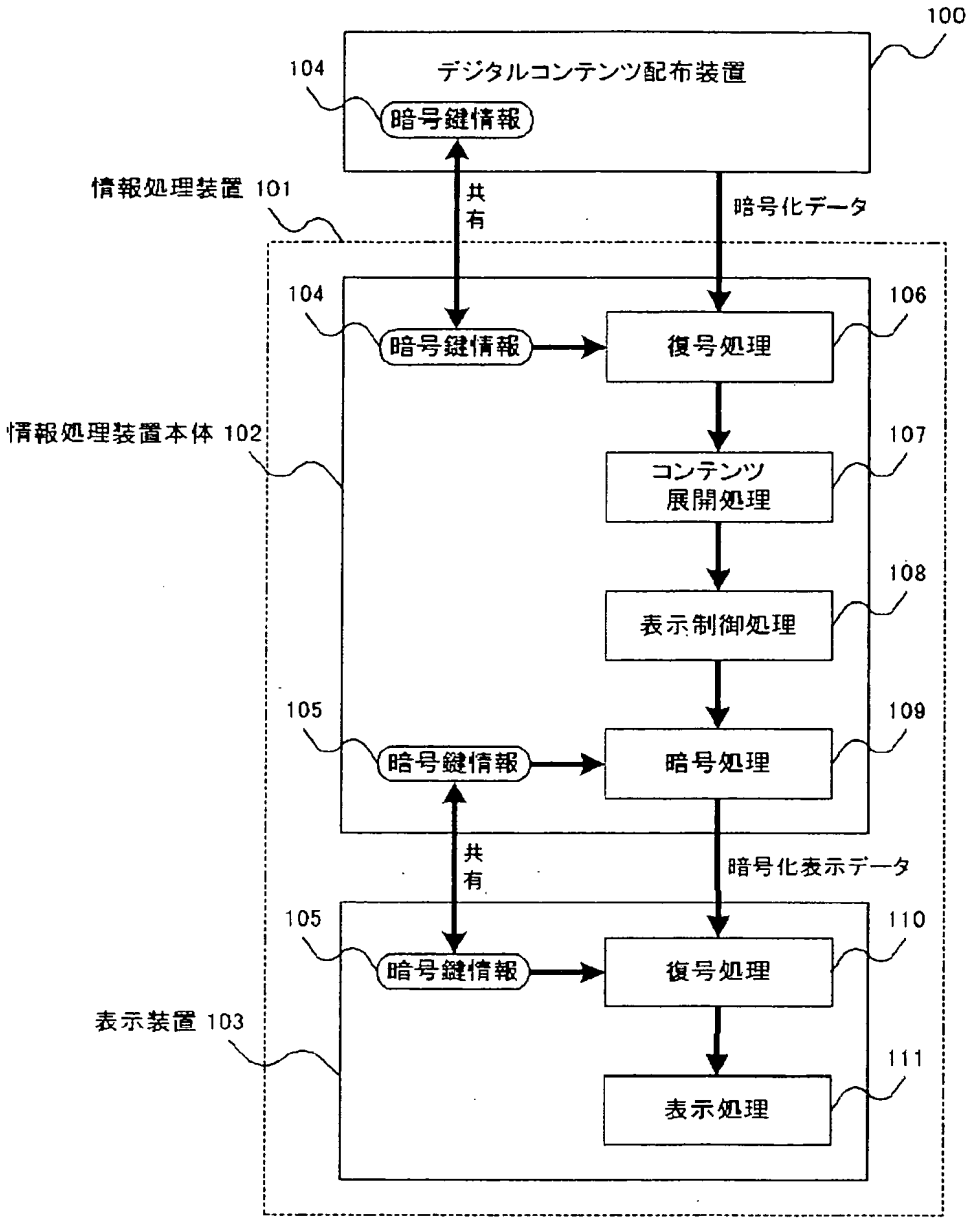
* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]

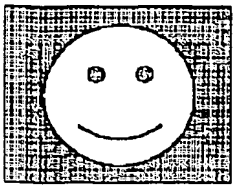
図 1


100
デジタルコンテンツ配布装置
104
暗号鍵情報
情報処理装置 101
共有
暗号化データ
104
暗号鍵情報
106
復号処理
情報処理装置本体 102
107
コンテンツ展開処理
108
表示制御処理
105
暗号鍵情報
109
暗号処理
共有
暗号化表示データ
105
暗号鍵情報
110
復号処理
表示装置 103
111
表示処理

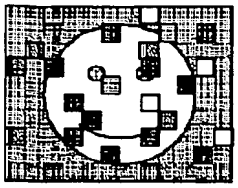
[Drawing 6]

図6

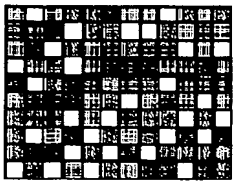
(a)



(b)

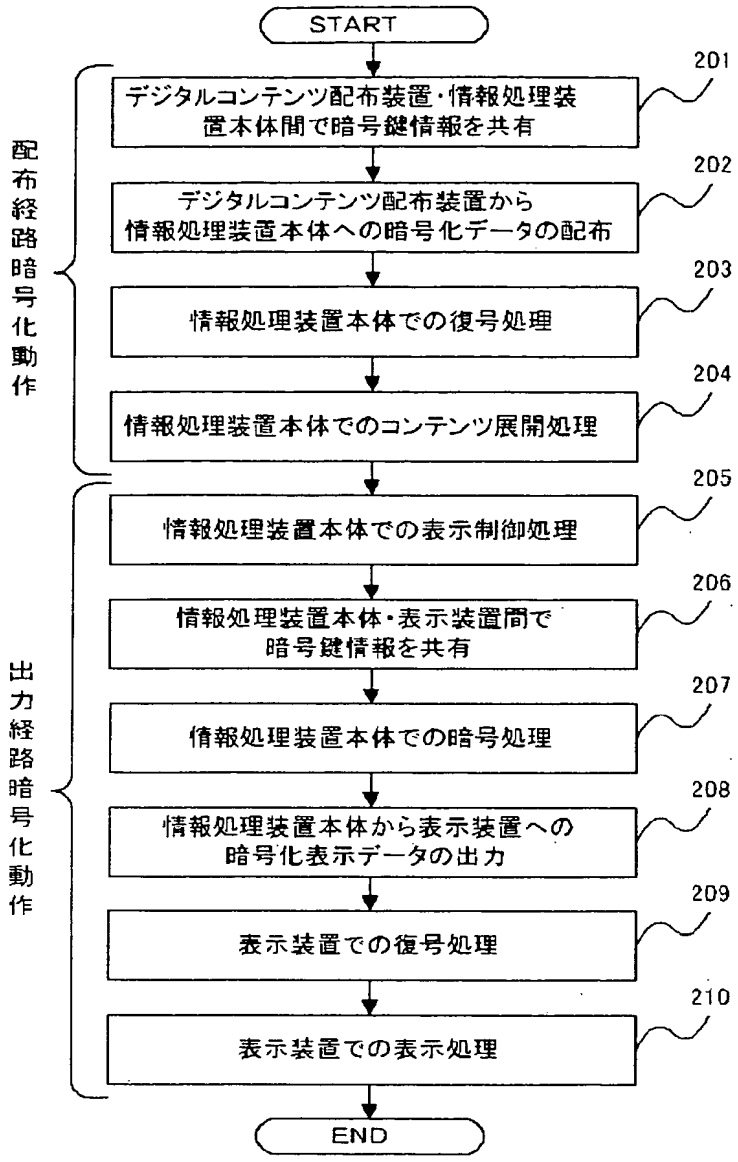


(c)



[Drawing 2]

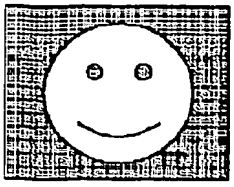
図 2



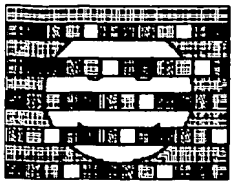
[Drawing 11]

図11

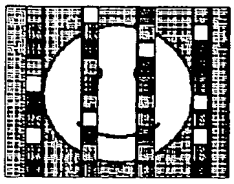
(a)



(b)



(c)



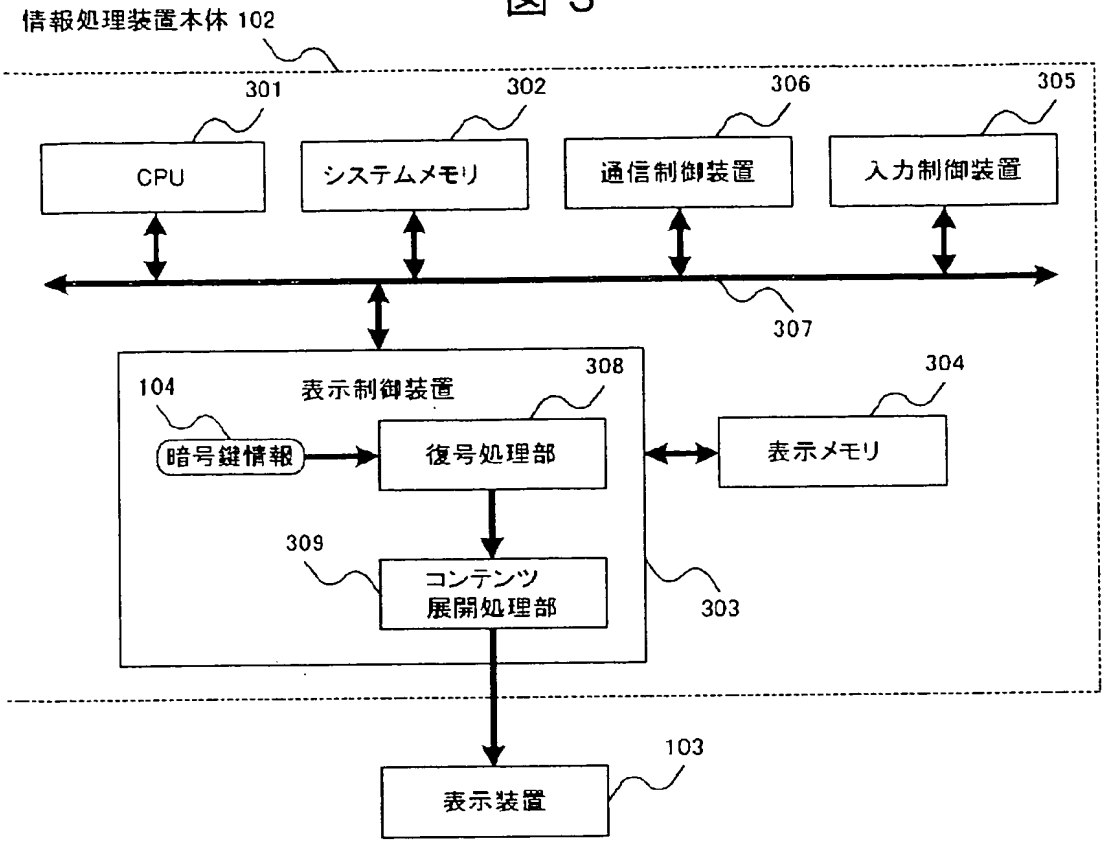
[Drawing 12]

図 12

	MBS							LBS	
平文	0	1	0	1	0	1	0	1	=55h
上位ビット暗号化	1	1	1	0	0	1	0	1	=e5h
下位ビット暗号化	0	1	0	1	0	0	1	0	=52h

[Drawing 3]

図 3



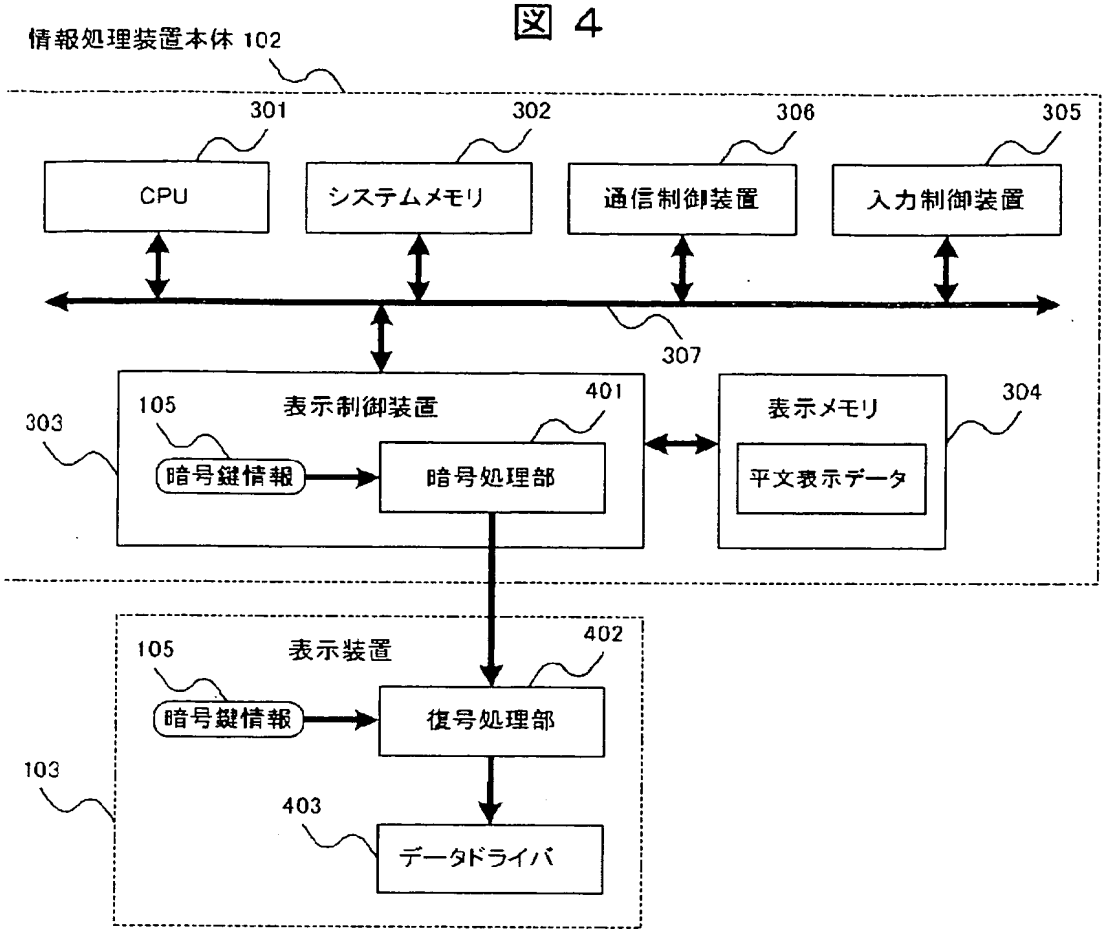
[Drawing 5]

図 5

暗号化対象	暗号鍵情報なしに得られるピクチャデータ			符号割り当て量@ピクチャデータ	暗号処理量@ピクチャデータ
	I	P	B		
Iピクチャデータ	×	×	×	大	大
Pピクチャデータ	○	×	×	中	中
Bピクチャデータ	○	○	×	小	小

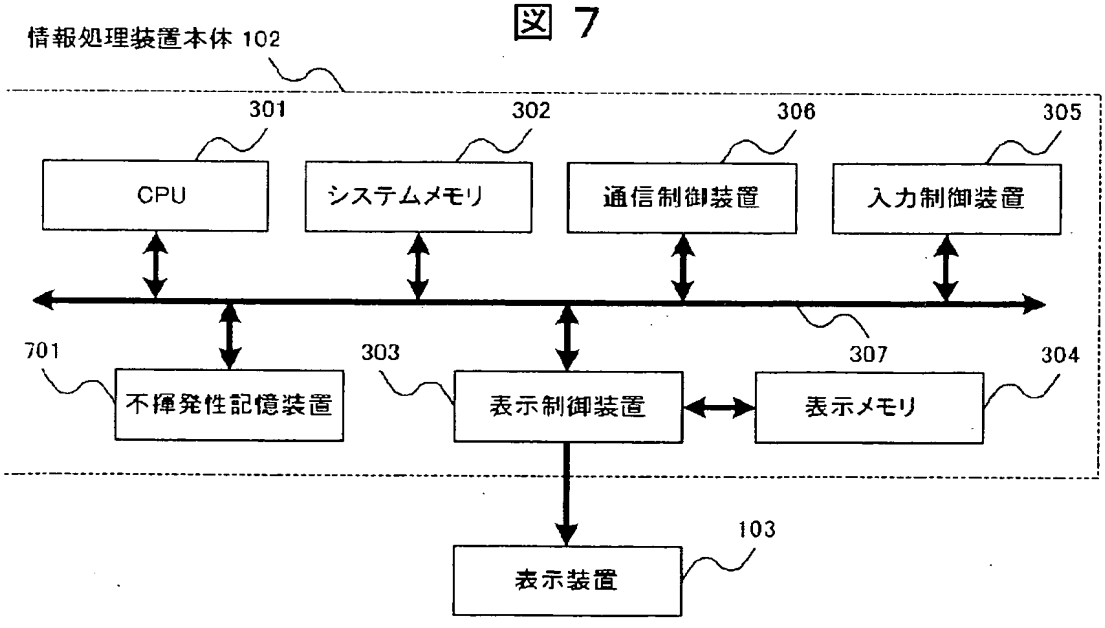
[Drawing 4]

図 4



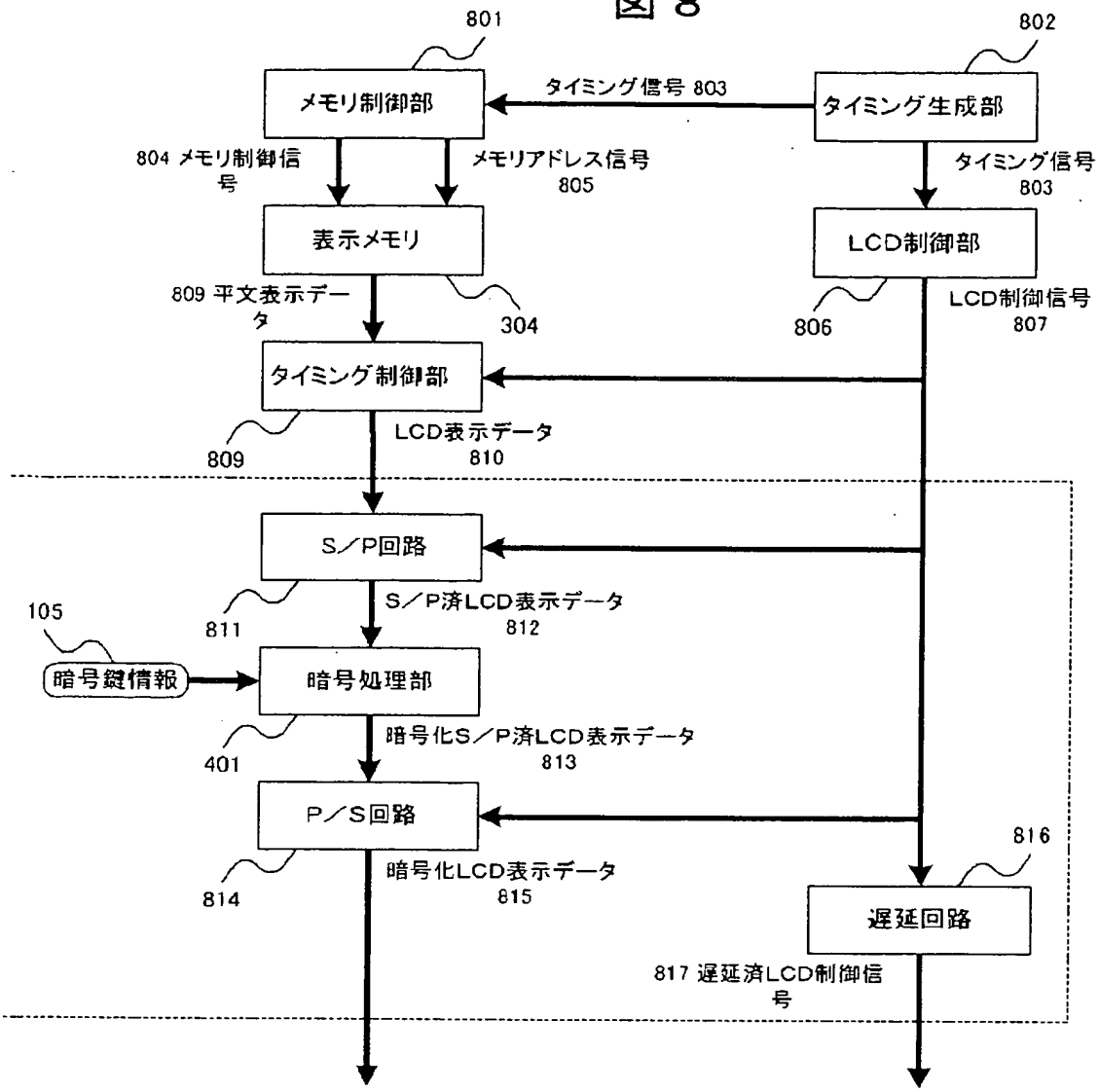
[Drawing 7]

図 7



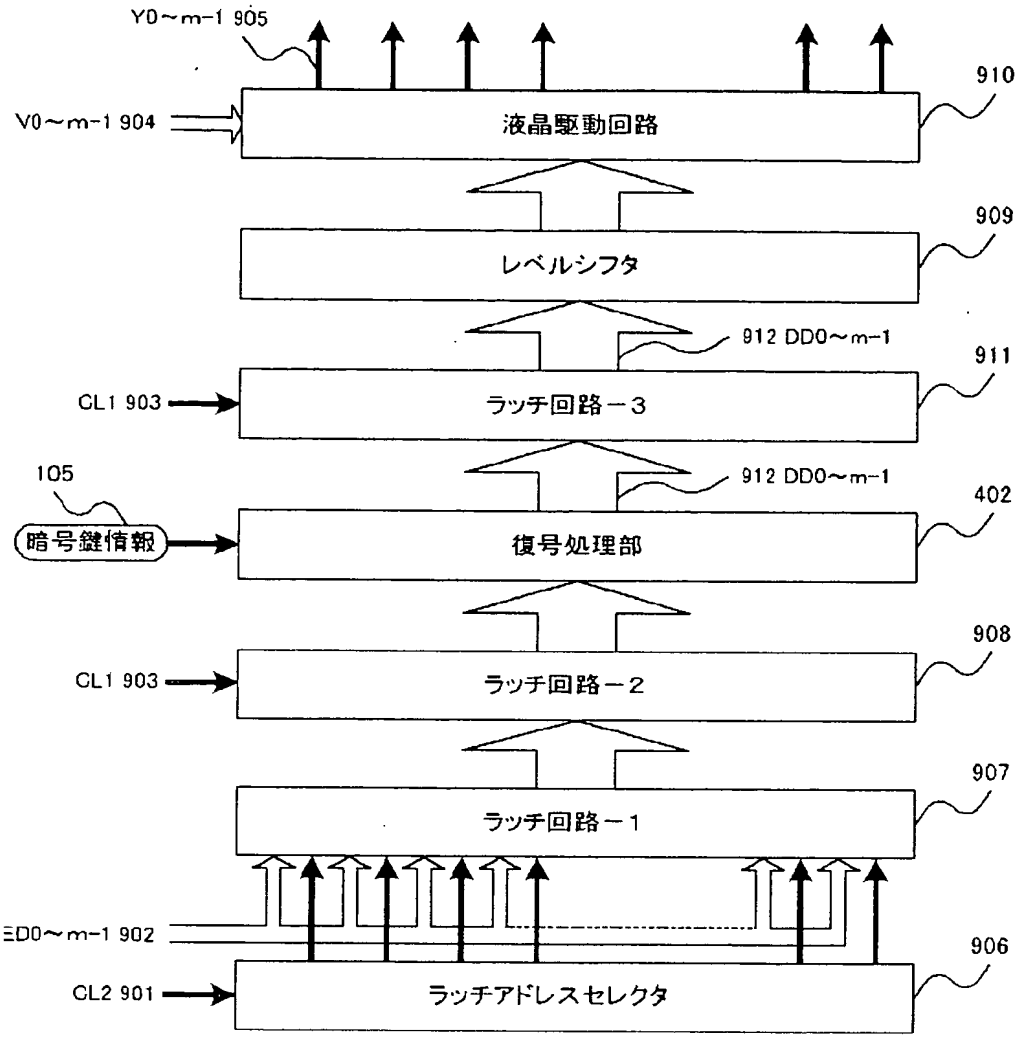
[Drawing 8]

図 8


801
802
メモリ制御部
タイミング信号 803
タイミング生成部
804 メモリ制御信号
メモリアドレス信号 805
タイミング信号 803
表示メモリ
LCD制御部
809 平文表示データ
304
806
LCD制御信号 807
タイミング制御部
809
LCD表示データ 810
S／P回路
105
811
S／P済LCD表示データ 812
暗号鍵情報
暗号処理部
401
暗号化S／P済LCD表示データ 813
P／S回路
816
814
暗号化LCD表示データ 815
遅延回路
817 遅延済LCD制御信号

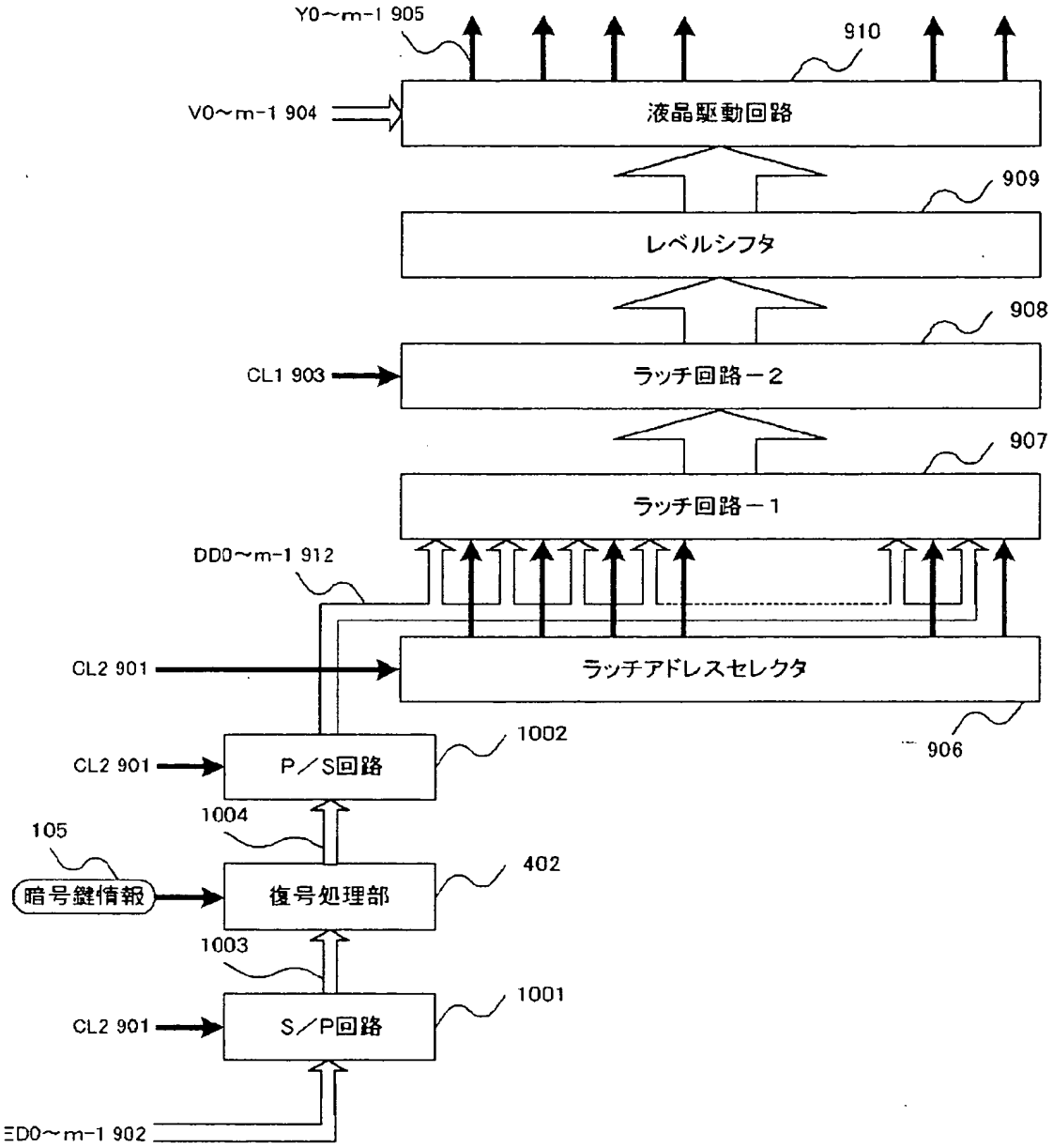
[Drawing 9]

図 9



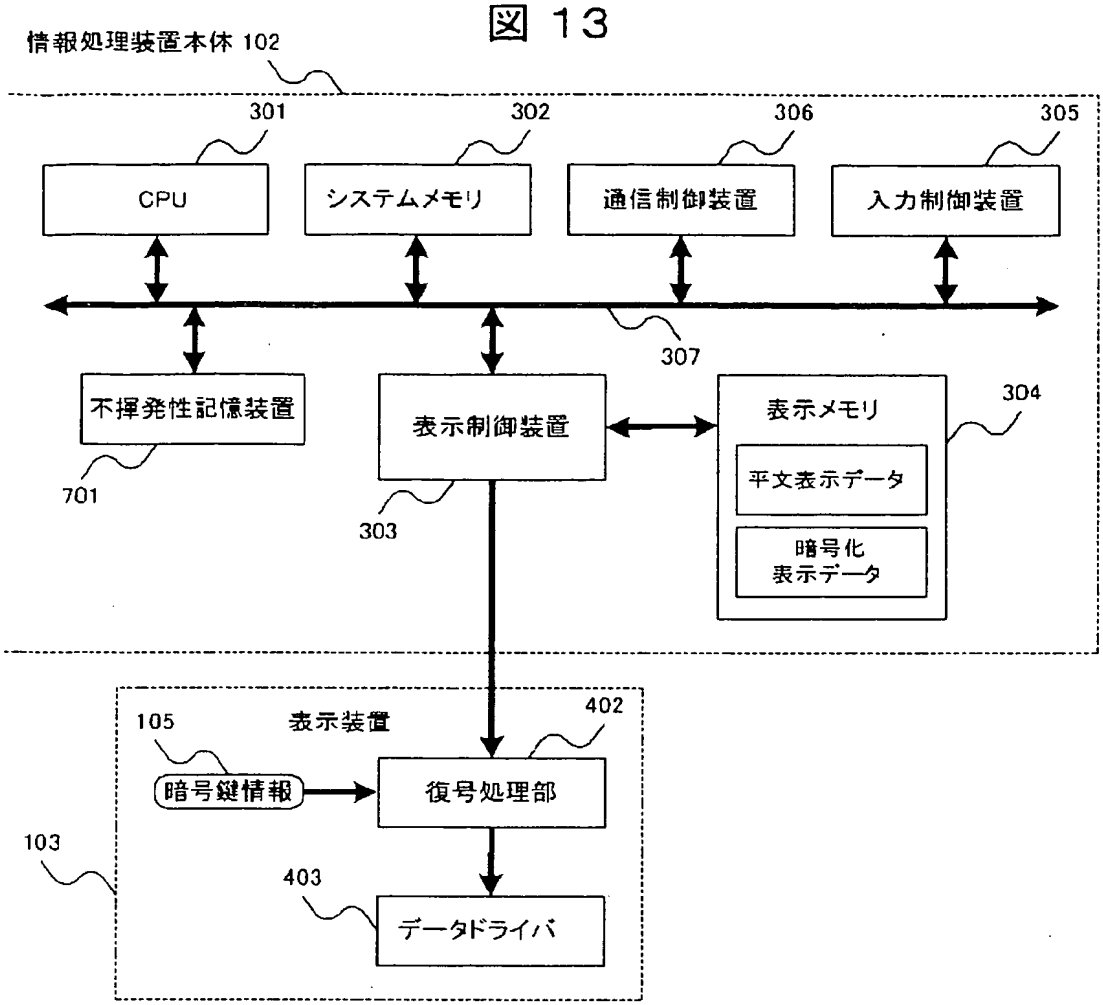
[Drawing 10]

図 10



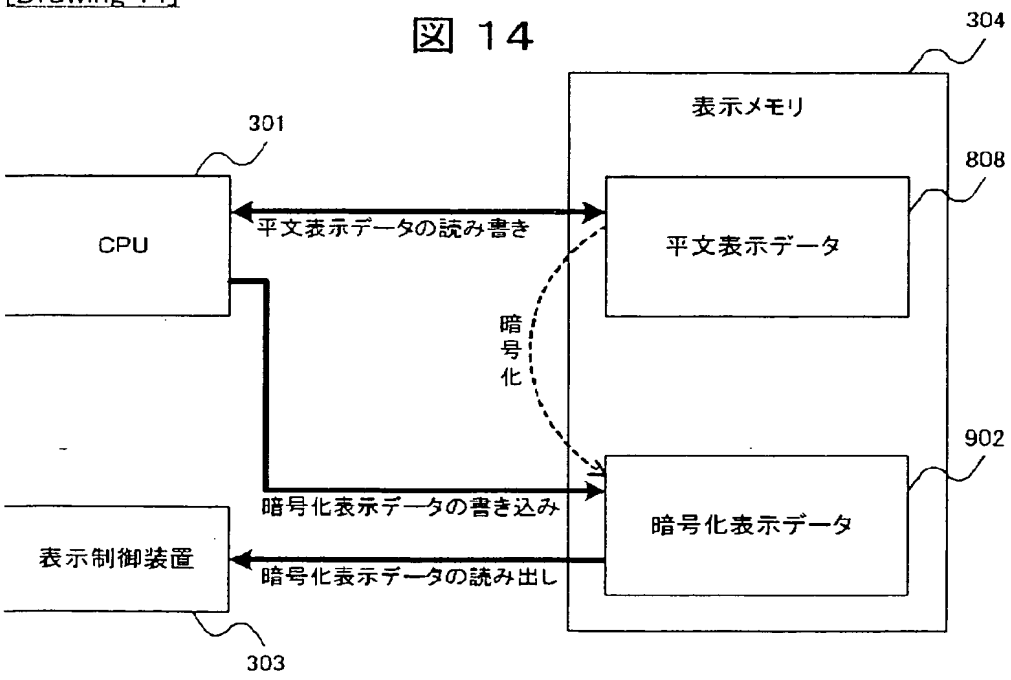
[Drawing 13]

図 13



[Drawing 14]

図 14



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－158654
（P2002－158654A）
(43)公開日　平成14年５月31日(2002.5.31)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード'（参考）
Ｈ０４Ｌ　9/16		Ｈ０４Ｌ　9/00	６４３	５Ｃ０６４
9/08			６０１Ｚ	５Ｊ１０４
Ｈ０４Ｎ　7/167			６０１Ｅ	
		Ｈ０４Ｎ　7/167	Ｚ	

審査請求　未請求　請求項の数14　ＯＬ　（全 23 頁）

(21)出願番号　特願2000－351510(P2000－351510)

(22)出願日　平成12年11月17日(2000.11.17)

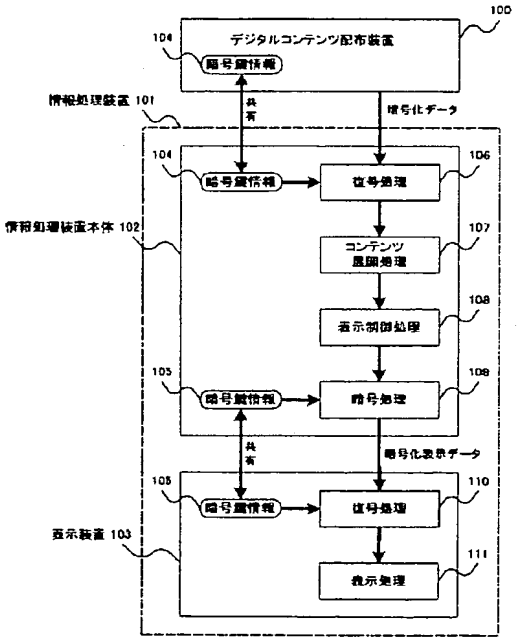
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　大和田　徹
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　北原　潤
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100084032
弁理士　三品　岩男　（外１名）

最終頁に続く

(54)【発明の名称】　情報処理装置、表示装置、デジタルコンテンツ配布システム、および、デジタルコンテンツ配布・出力方法

(57)【要約】
【課題】デジタルコンテンツの権利を保護しつつ、ユーザの視聴覚欲求を刺激する形でのデジタルコンテンツの最終出力を可能とする。
【解決手段】情報処理装置本体１０２が、表示装置１０３と共有する暗号鍵情報１０５を用いて暗号化したデジタルコンテンツ（表示データ）を、表示装置１０３に転送し、表示装置１０３が、情報処理装置本体１０２から転送される表示データに対して、暗号鍵情報１０５を用いてを用いて復号処理を施すようにしている。ここで、情報処理装置本体１０２から表示装置１０３に転送される表示データは、例えば、数ライン分おきに、数ライン分の表示データずつが暗号化されるなど、一部分のみが暗号化されたものである。

図１



1

【特許請求の範囲】
【請求項１】処理装置および出力装置を少なくとも備えた情報処理装置において、
上記処理装置は、
デジタルコンテンツに対して、上記出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え、
上記出力装置は、
上記処理装置から転送されるデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツに対して、上記処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたことを特徴とする情報処理装置。
【請求項２】処理装置および出力装置を少なくとも備えた情報処理装置において、
上記処理装置は、
デジタルコンテンツの一部分に対して、上記出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
一部分が暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え、
上記出力装置は、
上記処理装置から転送されるデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツに対して、上記処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたことを特徴とする情報処理装置。
【請求項３】処理装置および出力装置を少なくとも備えた情報処理装置において、
上記処理装置は、
暗号化されたデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツに対して、該デジタルコンテンツを復号するための暗号鍵情報を用いて復号処理を施す復号処理手段と、
復号後のデジタルコンテンツの一部分に対して、上記出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え、
上記出力装置は、
上記処理装置から転送されるデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツに対して、上記処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手

2

段と、
暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたことを特徴とする情報処理装置。
【請求項４】暗号化されたデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツに対して、該デジタルコンテンツを復号するための暗号鍵情報を用いて復号処理を施す復号処理手段と、
復号後のデジタルコンテンツの一部分に対して、該デジタルコンテンツの出力先の出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
一部分が暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備えたことを特徴とする情報処理装置。
【請求項５】請求項３または４記載の情報処理装置であって、
上記入力手段が入力するデジタルコンテンツは、
平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位の一部の単位が暗号化対象となるようにして暗号化されていることを特徴とする情報処理装置。
【請求項６】請求項２，３，４または５記載の情報処理装置であって、
上記暗号処理手段は、
平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。
【請求項７】請求項２，３，４または５記載の情報処理装置であって、
上記出力装置が音声再生装置である場合に、
上記暗号処理手段は、
上記音声再生装置に出力する音声データについて、複数サンプル分の音声データを１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。
【請求項８】請求項２，３，４または５記載の情報処理装置であって、
上記出力装置が表示装置である場合に、
上記暗号処理手段は、
上記表示装置に出力する表示データのライン方向に、複数ライン分の表示データを１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すか、または、上記表示装置に出力する表示データのカラム方向に、複数カラム分の表示データを１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。
【請求項９】請求項２，３，４または５記載の情報処理装置であって、
上記出力装置が表示装置である場合に、

上記暗号処理手段は、
上記表示装置に出力する表示データの１画素分のデータを１単位とし、これらの単位の一部または全部について、各々、その一部分を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。
【請求項１０】暗号化された表示データを入力する入力手段と、
入力した表示データに対して、該表示データの転送元の情報処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後の表示データを表示する表示手段とを備えたことを特徴とする表示装置。
【請求項１１】請求項１０記載の表示装置であって、
上記入力手段が入力するデジタルコンテンツは、
平文時の表示データのライン方向に、複数ライン分の表示データを１単位とし、これらの単位の一部の単位が暗号処理の処理対象となるようにして暗号化されているか、または、平文時の表示データのカラム方向に、複数カラム分の表示データを１単位とし、これらの単位の一部の単位が暗号処理の処理対象となるようにして暗号化されていることを特徴とする表示装置。
【請求項１２】請求項１０記載の情報処理装置であって、
上記入力手段が入力するデジタルコンテンツは、
平文時の表示データの１画素分のデータを１単位とし、これらの単位の一部または全部について、各々、その一部分が暗号処理の処理対象となるようにして暗号化されていることを特徴とする表示装置。
【請求項１３】デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力装置に転送して出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、
上記デジタルコンテンツ配布装置は、
上記情報処理装置と共有する第１の暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを蓄積している蓄積手段と、
蓄積しているデジタルコンテンツを上記情報処理装置に配布する配布手段とを備え、
上記情報処理装置は、
上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツ中の暗号化部分に対して、上記第１の暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後のデジタルコンテンツの一部分に対して、上記出力装置と共有する第２の暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え、

上記出力装置は、
上記情報処理装置から転送されるデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツ中の暗号化部分に対して、上記第２の暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備え、
上記デジタルコンテンツ配布装置の暗号処理手段、および、上記情報処理装置の暗号処理手段は、
平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とするデジタルコンテンツ配布システム。
【請求項１４】デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力装置に転送して出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、上記デジタルコンテンツ配布装置から上記情報処理装置へデジタルコンテンツを配布して上記出力装置で出力する方法であって、
上記デジタルコンテンツ配布装置が、上記情報処理装置と共有する第１の暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを、上記情報処理装置に配布し、
上記情報処理装置が、上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツ中の暗号化部分に対して、上記第１の暗号鍵情報を用いて復号処理を施し、暗号化部分を復号後のデジタルコンテンツの一部分に対して、上記出力装置と共有する第２の暗号鍵情報を用いて暗号処理を施してから、暗号化後のデジタルコンテンツを上記出力装置に転送し、
上記出力装置が、上記情報処理装置から転送されるデジタルコンテンツ中の暗号化部分に対して、上記第２の暗号鍵情報を用いて復号処理を施し、暗号化部分を復号後のデジタルコンテンツのを出力し、
上記デジタルコンテンツ配布装置が配布するデジタルコンテンツ、および、上記情報処理装置が転送するデジタルコンテンツは、
平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位中の一部の単位が暗号化対象となるようにして暗号化されていることを特徴とするデジタルコンテンツ配布・出力方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、著作権保護が必要なデジタルコンテンツを扱う技術に関し、特に、複製による不正使用を防ぎ、かつ、正当な使用権利を持たないユーザの視聴覚欲求を刺激する形での利用を可能としながら、デジタルコンテンツを配布し、配布先の情報処理

装置で出力する方法に関する。

【０００２】

【従来の技術】近年、映像や音声などの高付加価値な情報をデジタル形式で配布する要求が高まっており、デジタルコンテンツの著作権保護を図るために、不正コピーの防止が重要視されてきている。すなわち、デジタルコンテンツは、容易にコピーできる上、コピーしても品質が劣化しないので、既に不正コピーによる著作権の侵害等の弊害が生じてきている。

【０００３】コピー防止手段の１つとしては、一般に、デジタルコンテンツの暗号化が用いられており、正当な暗号鍵情報を入手したユーザのみが、暗号化されたデジタルコンテンツを復号し、その中身を確かめることができるようにしている。

【０００４】

【発明が解決しようとする課題】しかしながら、デジタルコンテンツを単純に暗号化した場合、暗号化されたデジタルコンテンツは、正当な暗号鍵情報がないと全く視聴することができなくなってしまう。

【０００５】これは、デジタルコンテンツが何らかのフォーマットに従ってフォーマッティングされているにも関わらず、フォーマットを無視した単純な暗号化が行われることにより、デジタルコンテンツのデータ構造が破壊されてしまい、デジタルコンテンツを再生するソフトウェアやハードウェアがデータ構造を全く解釈できなくなるからである。

【０００６】そこで、ユーザは、デジタルコンテンツを購入するなどして、正当な暗号鍵情報を入手しない限り、その中身を確かめることができず、ユーザにとってはデジタルコンテンツ購入の敷居が高くなってしまう。

【０００７】このような問題を解決するためには、デジタルコンテンツの権利保護を大前提にしつつも、ユーザの視聴覚欲求を刺激する形でデジタルコンテンツを配布するようにすることが好ましい。

【０００８】また、従来、デジタルコンテンツの暗号化は、ユーザの情報処理装置に到達するまでの経路についてのみ行われており、情報処理装置において、表示装置などの最終出力装置へ出力する際の経路については、暗号化による著作権保護の対象とはなっていない。

【０００９】近年、従来のＣＲＴ（Cathode-Ray Tube）表示装置のようなアナログ入力の最終出力装置に代わり、液晶表示装置のようなデジタル入力の最終出力装置が一般化しつつあることから、このような最終出力装置へ出力する際の経路で、デジタルコンテンツの不正コピーが行われる恐れがある。

【００１０】そこで、本発明の目的は、情報処理装置において、デジタルコンテンツを最終的に出力する際の経路での不正コピーを防止することを可能にすることにある。

【００１１】また、本発明のもう１つの目的は、情報処理装置において、デジタルコンテンツの権利を保護すると共に、ユーザの視聴覚欲求を刺激することにより、デジタル時コンテンツの配布または販売を促進することを可能にすることにある。

【００１２】

【課題を解決するための手段】上記目的を達成するために、本発明は、処理装置および出力装置を少なくとも備えた情報処理装置において、上記処理装置が、上記出力装置と共有する暗号鍵情報を用いて暗号化したデジタルコンテンツを、上記上記出力装置に転送し、上記出力装置が、上記処理装置から転送されるデジタルコンテンツに対して、上記暗号鍵情報を用いて復号処理を施すようにしている。

【００１３】そして、特に、本発明では、もう１つの目的を達成するために、上記処理装置から上記出力装置に転送されるデジタルコンテンツが、平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位の一部の単位が暗号化対象となるようにして暗号化されたものであるようにしている。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【００１５】図１は、本実施形態に係るデジタルコンテンツ配布システムの概略構成図である。

【００１６】図中、１００はデジタルコンテンツ配布装置、１０１は情報処理装置、１０２は情報処理装置本体、１０３は表示装置である。

【００１７】本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツ配布装置１００によってデジタルデータとして配布される高付加価値コンテンツの権利保護を大前提としている。すなわち、本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツ配布装置１００と情報処理装置本体１０２との間を転送されるデジタルコンテンツ（配布データ）、および、情報処理装置本体１０２と表示装置１０３との間を転送されるデジタルコンテンツ（表示データ）が、各々、デジタルデータであるようなものを対象にしており、これらを暗号化することで保護を図っている。

【００１８】そして、本実施形態に係るデジタルコンテンツ配布システムは、ユーザの視聴覚欲求を刺激する形でデジタルコンテンツを配布可能とすることを目的としている。すなわち、本実施形態に係るデジタルコンテンツ配布システムは、暗号化されたデジタルコンテンツで、ユーザの視聴覚要求を刺激することを可能とするものである。

【００１９】具体的には、デジタルコンテンツ配布装置１００と情報処理装置本体１０２との間を転送されるデジタルコンテンツは、例えば、ＪＰＥＧ（Joint Photographic Experts Group）やＭＰＥＧ（Moving Picture Experts Group）などの、予め決められた圧縮方式でフォ

ーマッティングされたデジタルデータが、例えば、ＤＥＳ（Data Encryption Standard）などの、予め決められた暗号方式で暗号化された暗号化データである。

【００２０】ここで、デジタルコンテンツ配布装置１００は、ネットワークを経由してデジタルコンテンツを配布するネットワーク装置であっても、例えば、光ディスク媒体や磁気ディスク媒体などの、デジタルコンテンツが記録された記録媒体であってもよい。

【００２１】すなわち、デジタルコンテンツ配布装置１００によって配布されるデジタルコンテンツは、デジタルコンテンツ配布装置１００から配布される時点で暗号化されていればよく、暗号処理を施すのがデジタルコンテンツ配布装置１００でなくてもよい。

【００２２】さて、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、デジタルコンテンツ配布装置１００および情報処理装置本体１０２は、何らかの方法によって、デジタルコンテンツ（配布データ）を暗号化／復号化するための暗号鍵情報１０４を共有する機能を有している。

【００２３】暗号鍵情報１０４を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよい。

【００２４】例えば、デジタルコンテンツの暗号化に用いられた暗号鍵情報１０４を管理しているネットワーク装置から、情報処理装置本体１０２が暗号鍵情報１０４を入手するという方法が挙げられる。このとき、ネットワーク装置が、情報処理装置本体１０２の公開鍵情報を用いて暗号鍵情報１０４を暗号化し、情報処理装置本体１０２が、自身の秘密鍵情報で復号するようにする。

【００２５】また、例えば、磁気ディスク媒体に記録されているデジタルコンテンツ（暗号化済み）の暗号化に用いられた暗号鍵情報１０４を、情報処理装置本体１０２の製造時に、情報処理装置本体１０２の内部の不揮発性記憶装置に記録しておくという方法が挙げられる。

【００２６】同様に、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、情報処理装置本体１０２および表示装置１０３は、何らかの方法によって、デジタルコンテンツ（表示データ）を暗号化／復号化するための暗号鍵情報１０５を共有する機能を有している。

【００２７】暗号鍵情報１０５を共有する方法についても、暗号鍵情報１０４を共有する方法と同様に、様々な方法が公知技術となっており、どのような方法を採用してもよい。

【００２８】例えば、情報処理装置本体１０２がデジタルコンテンツの暗号化に用いた暗号鍵情報１０５を、表示装置１０３が情報処理装置本体１０２から入手するという方法が挙げられる。このとき、情報処理装置本体１０２が、表示装置１０３の公開鍵情報を用いて暗号鍵情報１０５を暗号化し、表示装置１０３が、自身の秘密鍵情報で復号するようにする。

【００２９】また、例えば、暗号鍵情報１０５を、情報処理装置本体１０２および表示装置１０３の製造時に、各々の内部の不揮発性記憶装置に記録しておくという方法が挙げられる。

【００３０】また、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、情報処理装置本体１０２は、（１）デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４を用いて復号処理１０６を施す復号機能、（２）暗号化部分を復号後のデジタルコンテンツの展開処理１０７を行う展開機能、（３）展開したデジタルコンテンツを、表示装置１０３が要求するビットレートで出力するための表示データに変換する表示制御処理１０８を行う表示制御機能、（４）表示データの一部分に対して、暗号鍵情報１０５を用いて暗号処理１０９を施す暗号機能、を有している。

【００３１】また、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、表示装置１０３は、（１）情報処理装置本体１０２の暗号機能によって暗号化された表示データ中の暗号化部分に対して、暗号鍵情報１０５を用いて復号処理１１０を施す復号機能、（２）暗号化部分を復号後の表示データの表示処理１１１を行う表示機能、を有している。

【００３２】次に、本実施形態に係るデジタルコンテンツ配布システムの概略動作について、図２を用いて説明する。

【００３３】図２は、本実施形態に係るデジタルコンテンツ配布システムの概略動作フローチャートである。

【００３４】図２において、まず、デジタルコンテンツ配布装置１００および情報処理装置本体１０２は、何らかの方法によって、デジタルコンテンツ（配布データ）を暗号化／復号化するための暗号鍵情報１０４を共有する（ステップ２０１）。上述したように、暗号鍵情報１０４を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよいので、ここでは規定しない。

【００３５】続いて、デジタルコンテンツ配布装置１００は、情報処理装置本体１０２へ、暗号鍵情報１０４を用いて一部分が暗号化されたデジタルコンテンツを配布する（ステップ２０２）。上述したように、デジタルコンテンツ配布装置１００によって配布されるデジタルコンテンツは、デジタルコンテンツ配布装置１００から配布される時点で暗号化されていればよく、暗号処理を施すのがデジタルコンテンツ配布装置１００でなくてもよい。

【００３６】続いて、情報処理装置本体１０２は、デジタルコンテンツ配布装置１００から配布されたデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４を用いて復号処理１０６を施す（ステップ２０３）。ス

テップ２０３の処理によって、情報処理装置本体１０２は、その内部に、平文のデジタルコンテンツを得ることとなる。

【００３７】続いて、情報処理装置本体１０２は、ステップ２０３の処理で得られたデジタルコンテンツの展開処理１０７を行う（ステップ２０４）。例えば、ステップ２０３の処理で得られたデジタルコンテンツがＭＰＥＧ方式でフォーマッティングされているＭＰＥＧデータである場合には、ステップ２０４の処理によって、情報処理装置本体１０２は、その内部に、毎秒３０フレームからなる動画像データを得ることとなる。

【００３８】続いて、ステップ２０４の処理で得られた動画像データを含む表示データに対して、表示装置１０３が要求するビットレートで出力するための表示制御処理１０８を行う（ステップ２０５）。例えば、表示装置１０３がＴＦＴ（Thin FilmTransistor）液晶表示装置の場合は、ステップ２０５の処理では、情報処理装置本体１０２は、毎秒６０～７０フレーム程度のシーケンシャルな表示データを生成する。

【００３９】続いて、情報処理装置本体１０２および表示装置１０３は、何らかの方法によって、デジタルコンテンツ（表示データ）を暗号化／復号化するための暗号鍵情報１０５を共有する（ステップ２０６）。上述したように、暗号鍵情報１０５を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよいので、ここでは規定しない。

【００４０】続いて、情報処理装置本体１０２は、ステップ２０５の処理で生成した表示データ中の一部分に対して、暗号鍵情報１０５を用いて暗号処理１０９を施す（ステップ２０７）。ステップ２０７の処理によって、情報処理装置本体１０２は、その内部に、一部分が暗号化された表示データを得ることとなる。

【００４１】続いて、情報処理装置本体１０２は、表示装置１０３へ、一部分が暗号化された表示データを出力する（ステップ２０８）。

【００４２】続いて、表示装置１０３は、情報処理装置本体１０２から出力された表示データ中の暗号化部分に対して、暗号鍵情報１０５を用いて復号処理１１０を施す（ステップ２０９）。ステップ２０９の処理によって、表示装置１０３は、その内部に、平文の表示データを得ることとなる。

【００４３】続いて、表示装置１０３は、ステップ２０９の処理によって得られた表示データの表示処理１１１を行う（ステップ２１０）。ステップ２１０の処理によって、ステップ２０４の処理によって得られた動画像データを含む表示データが表示されることとなる。

【００４４】以上、ステップ２０１～ステップ２１０の処理によって、デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツが、表示装置１０３で表示されることとなる。

【００４５】なお、以下では、本実施形態に係るデジタルコンテンツ配布システムの動作のうち、ステップ２０１～ステップ２０４の処理によって実現される動作を、「配布経路暗号化」動作と称し、ステップ２０５～ステップ２１０の処理によって実現される動作を、「出力経路暗号化」動作と称する。

【００４６】また、ステップ２０６の処理は、配布経路暗号化動作に先立って行われても、並行して行われてもよい。また、ステップ２０５，ステップ２０６，ステップ２０７の処理は、情報処理装置１０１の構成によっては順番が逆転してもよい。

【００４７】次に、配布経路暗号化動作の詳細について説明する。

【００４８】まず、本実施形態に係る情報処理装置１０１の概略動作について、図３を用いて説明する。

【００４９】図３は、本実施形態に係る情報処理装置１０１の概略構成図である。

【００５０】図３では、パーソナルコンピュータ（ＰＣ）などの情報処理装置１０１のうち、表示に関する部分であって、かつ、配布経路暗号化動作に関する部分のみを示している。

【００５１】図中、１０２は情報処理装置本体、１０３は表示装置、１０４は暗号鍵情報、３０１は中央演算装置（ＣＰＵ：Central Processing Unit）、３０２はシステムメモリ、３０３は表示制御装置、３０４は表示メモリ、３０５は入力制御装置、３０６は通信制御装置、３０７はバス、３０８は復号処理部、３０９はコンテンツ展開処理部である。

【００５２】図３において、デジタルコンテンツ配布装置１００がネットワーク装置である場合には、通信制御装置３０６が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。また、デジタルコンテンツ配布装置１００が記録媒体である場合には、入力制御装置３０５が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。通信制御装置３０６または入力制御装置３０５が入力したデジタルコンテンツは、ＣＰＵ３０１の指示に従って、バス３０７を介して表示制御装置３０３に入力される。

【００５３】表示制御装置３０３においては、復号処理部３０８が、入力したデジタルコンテンツ中の暗号化部分に対して、表示制御装置３０３の内部に保持されている暗号鍵情報１０４を用いて復号処理１０６を施し、表示制御装置３０３の内部に、平文のデジタルコンテンツを得る。続いて、コンテンツ展開処理部３０９が、復号処理部３０８が復号したデジタルコンテンツの展開処理１０７を行い、表示制御装置３０３の内部に、展開されたデジタルコンテンツを得る。

【００５４】ここまでの動作が配布経路暗号化動作に相当している。その後の出力経路暗号化動作の詳細については後述する。

【００５５】なお、復号処理部３０８およびコンテンツ展開処理部３０９は、表示制御装置３０３内にハードウェアとして実装されるようにしてもよいし、また、表示制御装置３０３内に独自のＣＰＵおよびメモリを設け、ソフトウェアとして実装されるようにしてもよい。

【００５６】次に、配布経路暗号化動作で、デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツの暗号化方法の一例について、図５および図６を用いて説明する。

【００５７】図５は、デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツの暗号化方法の一例を示す説明図であり、図６は、図５に示す暗号化方法で暗号化されたデジタルコンテンツを表示装置１０３で表示した場合の表示イメージを示す説明図である。

【００５８】図５および図６では、デジタルコンテンツがＭＰＥＧデータである場合を例にしている。

【００５９】ＭＰＥＧ方式による圧縮では、例えば、１フレームｍ×ｎ画素，毎秒ｋフレームから構成される動画像データは、Ｉピクチャ形式，Ｐピクチャ形式，Ｂピクチャ形式の３つの形式に分類される。

【００６０】（１）Ｉピクチャ形式

Ｉピクチャ形式では、１フレームｍ×ｎ画素の画像データは、８×８画素の複数のブロックに分割され、各ブロックごとに直交変換処理が施されて周波数領域データに変換された後、量子化されてデータ圧縮が行われる。Ｉピクチャデータでは、元フレーム内のデータのみを対象にした符号化がなされており、Ｉピクチャデータからは、展開処理によって１枚のフレームデータが得られる。

【００６１】（２）Ｐピクチャ形式

Ｐピクチャ形式では、順方向のフレーム間予測を行ったデータ圧縮が行われる。Ｐピクチャデータでは、Ｉピクチャとの差分情報を用いた符号化がなされており、元フレームの復元には、Ｐピクチャデータ，元画となるＩピクチャデータが必要となる。すなわち、Ｐピクチャデータのみでは画像データは得られない。

【００６２】（３）Ｂピクチャ形式

Ｂピクチャ形式では、双方向のフレーム間予測を行ったデータ圧縮が行われる。Ｂピクチャデータでは、ＩピクチャとＰピクチャとの間の差分情報を用いた符号化がなされており、元フレームの復元には、Ｐピクチャデータ，元画となるＩピクチャデータ，Ｂピクチャデータが必要となる。すなわち、Ｂピクチャデータのみでは画像データは得られない。

【００６３】また、Ｉピクチャデータの符号割り当て量は、図５に示すように、Ｉピクチャ，Ｐピクチャ，Ｂピクチャの順に小さくなる。動画像データは、フレームごとに、例えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢなどの順番に符号化される。

【００６４】このような性質を持ったＭＰＥＧデータの暗号化方法としては、以下の３つの方法が考えられる。

【００６５】（１）第１の暗号化方法

第１の暗号化方法としては、Ｉピクチャデータのみを暗号化するという方法がある。第１の暗号化方法は、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

【００６６】まず、前者の方法（圧縮単位となるブロックごとに暗号化を施す／施さないという方法）について説明すると、例えば、図６（ａ）に示す元画像に対して、本方法による暗号化を行う際には、ブロックを暗号処理の処理対象とし、あるブロックには暗号処理を施し、あるブロックには暗号処理を施さないようにする。

【００６７】本方法により暗号化されたＭＰＥＧデータは、暗号鍵情報１０４を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図６（ｂ）に示すようになる。本方法では、暗号化を施すブロック数を増減させることで、元画像の汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【００６８】次に、後者の方法（高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法）について説明すると、例えば、図６（ａ）に示す元画像に対して、本方法による暗号化を行う際には、ブロック内の低周波領域データを暗号処理の処理対象とし、各ブロック中の低周波領域データには暗号処理を施し、高周波領域データには暗号処理を施さないようにする。本方法により暗号化されたＭＰＥＧデータは、暗号鍵情報１０４を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図６（ｃ）に示すようになる。

【００６９】低周波数領域データを暗号化すると、図６（ｃ）に示すように、元画像は大きく汚染され、元画像を観測するのは困難となるが、高周波数領域データを暗号化すると、図示していないが、元画像にノイズが重畳されたイメージとなる。

【００７０】本方法では、暗号化を施す周波数領域を選択することで、元画像の汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。また、全てのブロックを暗号処理の処理対象としなくても、一部のブロックを暗号処理の処理対象としてもよい。

【００７１】第１の暗号化方法によってＩピクチャデータのみを暗号化した場合、暗号鍵情報１０４がないとＩピクチャデータを復元することができず、従って、図５に示すように、Ｉピクチャデータの差分情報であるＰピクチャデータおよびＢピクチャデータも、暗号化されてはいないが、これらを展開することも不可能となる。例

えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢの順番に符号化された動画像データは、暗号鍵情報１０４がない場合には、×××，×××，×××，×××，×××，×××（×は正常な復号・展開の失敗を意味する。）となって、全てのフレーム共に正常な元画像が得られない。

【００７２】（２）第２の暗号化方法

第２の暗号化方法としては、Ｐピクチャデータのみを暗号化するという方法がある。第２の暗号化方法も、第１の暗号化方法と同様に、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

【００７３】第２の暗号化方法によってＰピクチャデータのみを暗号化した場合、暗号鍵情報１０４がないとＰピクチャデータを復元することができず、従って、図５に示すように、Ｉピクチャデータ，Ｐピクチャデータの差分情報であるＢピクチャデータも、暗号化されてはいないが、これを展開することも不可能となる。例えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢの順番に符号化された動画像データは、暗号鍵情報１０４がない場合には、Ｉ××，×××，×××，Ｉ××，×××，×××（×は正常な復号・展開の失敗を意味する。）となって、得られる正常な画像フレームはＩピクチャデータのみとなる。

【００７４】（３）第３の暗号化方法

第３の暗号化方法としては、Ｂピクチャデータのみを暗号化するという方法がある。第３の暗号化方法も、第１の暗号化方法と同様に、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

【００７５】第３の暗号化方法によってＢピクチャデータのみを暗号化した場合、図５に示すように、暗号鍵情報１０４がないとＢピクチャデータを復元することができない。例えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢの順番に符号化された動画像データは、暗号鍵情報１０４がない場合には、Ｉ××，Ｐ××，Ｐ××，Ｉ××，Ｐ××，Ｐ××（Ｘは正常な復号・展開の失敗を意味する。）となって、得られる正常な画像フレームはＩピクチャデータおよびＰピクチャのみとなる。

【００７６】以上、ＭＰＥＧデータの暗号化方法として３つの方法を説明したが、これらの方法を任意に組み合わせるようにしてもよい。

【００７７】本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、デジタルコンテンツを単純に暗号化するのではなく、暗号処理の処理対象とするデータを選択し、一部分のみを暗号化するようにしているので、正当な暗号鍵情報１０４を有していない場合には、元画像の一部分が汚損した状態となる。一部分が汚損されたデジタルコンテンツは、その価値が損なわれるので、デジタルコンテンツの不正コピーを防止することが可能となり、また、デジタルコンテンツの一部分が開示されるので、ユーザの視聴要求を刺激し、デジタルコンテンツの完全な視聴を促すことが可能となる。

【００７８】特に、本実施形態に係るデジタルコンテンツ配布システムにおいては、暗号処理の処理対象とするデータを選択する際に、そのフォーマットに着目するようにしている。すなわち、デジタルコンテンツを単なるビット列として暗号処理の処理対象とした場合、ヘッダ，ペイロード，フッタと言ったデータ構造が全て失われてしまい、デジタルコンテンツとして利用することがまったく不可能となってしまうが、本実施形態に係るデジタルコンテンツ配布システムにおいては、デジタルコンテンツを単なるビット列として扱うのではなく、暗号処理の処理対象とするデータを、フォーマットの有意味部分に合わせて選択するようにしているので、データ全体ではなく、一部分だけの汚損が可能となっている。

【００７９】また、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、データ汚損に、暗号鍵情報１０４を用いた暗号処理を利用していることから、ユーザの視聴欲求を刺激するために、完全なデジタルコンテンツとは別に汚損デジタルコンテンツを用意する必要がなく、デジタルコンテンツの配布・蓄積に掛かるコストを低減することが可能となる。

【００８０】さらに、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、デジタルコンテンツの一部分だけを暗号処理の処理対象とし、デジタルコンテンツ全体に対する暗号処理を避けることによって、暗号処理／復号処理の処理量の軽減も可能となっている。なお、汚損度と処理量とはトレードオフの関係にあり、要求に応じて優先度の変更が容易に可能である。

【００８１】以上説明したように、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作によって、デジタルコンテンツの配布経路上で著作権を保護しつつ、ユーザの視聴欲求を刺激することが可能となる。

【００８２】なお、本実施形態に係る情報処理装置１０１は、図３に示す構成ではなく、図７に示す構成にし、図３に示した復号処理部３０８およびコンテンツ展開処理部３０９を、ソフトウェアで実現するようにしてもよい。

【００８３】図７は、本実施形態に係る情報処理装置１０１の他の概略構成図である。

【００８４】図７でも、図３と同様に、ＰＣなどの情報

処理装置１０１のうち、表示に関する部分であって、かつ、配布経路暗号化動作に関する部分のみを示している。

【００８５】図中、図３と同じ構成要素には同じ符号を付与してある。７０１は不揮発性記憶装置である。

【００８６】図７に示す構成の情報処理装置１０１においては、図３に示した復号処理部３０８およびコンテンツ展開処理部３０９の動作を、ＣＰＵ３０１がシステムメモリ３０２上にプログラムをロードして実行することで実現するものである。

【００８７】図７において、デジタルコンテンツ配布装置１００がネットワーク装置である場合には、通信制御装置３０６が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。また、デジタルコンテンツ配布装置１００が記録媒体である場合には、入力制御装置３０５が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。通信制御装置３０６または入力制御装置３０５が入力したデジタルコンテンツは、ＣＰＵ３０１の指示に従って、バス３０７を介してシステムメモリ３０２に入力される。

【００８８】ＣＰＵ３０１は、入力したデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４を用いて復号処理１０６を施し、システムメモリ３０２上に、平文のデジタルコンテンツを得る。続いて、ＣＰＵ３０１は、復号したデジタルコンテンツの展開処理１０７を行い、展開されたデジタルコンテンツを得る。得られたデジタルコンテンツは表示制御装置３０３に入力される。

【００８９】ここで、暗号鍵情報１０４は、図３を用いた説明では、表示制御装置３０３の内部に保持されているものとしたが、図７に示す構成の情報処理装置１０１においては、暗号鍵情報１０４の共有も、ＣＰＵ３０１がシステムメモリ３０２上にプログラムをロードして実行することで実現するものとする。

【００９０】また、本実施形態に係る情報処理装置１０１は、図３および図７のいずれにおいても、情報処理装置１０２本体と表示装置１０３とを備えた構成としているが、情報処理装置本体１０２と表示装置１０３が一体化した構成であってもよい。すなわち、本実施形態に係る情報処理装置１０１を、いわゆるＰＤＡ（PersonalDigital Assistant）などと呼ばれる携帯情報端末としてもよい。

【００９１】一般に、携帯情報端末は、比較的性能の低いＣＰＵや小容量のメモリなどを用いて構成されることが多いので、比較的重い処理である暗号処理は携帯情報端末にとって大きな負担になるという問題がある。

【００９２】そこで、このような問題がある携帯情報端末を、本実施形態に係るデジタルコンテンツ配布システムで用いるようにすれば、全体ではなく一部分が暗号化されたデジタルコンテンツを扱うことにより、本発明が

目的とする、著作権保護とユーザの視聴覚欲求刺激の両立を実現することができる上、暗号処理量の低減による負荷低下効果を得ることができる。特に、携帯情報端末が暗号処理をソフトウェアで実現する場合には、暗号処理用に高性能なＣＰＵや大容量メモリを搭載する必要がなくなり、低コスト化，低消費電力化といった効果が得られる。また、携帯情報端末が暗号処理専用のハードウェアを備えるようにする場合には、暗号処理専用のハードウェアに必要な処理速度が低下することから、低動作速度による低消費電力化，ハードウェア論理の小規模化による低コスト化といった効果が得られる。

【００９３】ところで、上述の説明では、ＭＰＥＧデータ（動画像データ）を例にしたが、必ずしも動画像データのみを対象としている訳ではない。

【００９４】例えば、デジタルコンテンツがＪＰＥＧデータ（静止画像データ）である場合には、上述したＩピクチャデータの暗号化方法と同様の暗号化方法を用いることが可能である。

【００９５】また、例えば、デジタルコンテンツがＭＰＥＧデータ（音声データ）である場合には、音声情報に対して帯域分割を施し、分割された周波数成分ごとに独立した符号化を行っていることから、低周波成分のみに対する暗号化／高周波成分のみに対する暗号化を行うようにしたり、数サンプルおきに暗号化を行うようしたりすればよい。このようにしてデータ汚損度を制御すれば、適度に耳障りな再生音を生成することが可能となる。

【００９６】さて、次に、出力経路暗号化動作の詳細について説明する。

【００９７】まず、本実施形態に係る情報処理装置１０１の概略動作について、図４を用いて説明する。

【００９８】図４は、本実施形態に係る情報処理装置１０１の概略構成図である。

【００９９】図４では、ＰＣなどの情報処理装置１０１のうち、表示に関する部分であって、かつ、出力経路暗号化動作に関する部分のみを示している。

【０１００】図中、図３と同じ構成要素には同じ符号を付与してある。４０１は暗号処理部、４０２は復号処理部、４０３はデータドライバである。

【０１０１】ここでは、表示装置１０３は、例えば、液晶表示（ＬＣＤ：Liquid Crystal Display）装置や、デジタル／アナログ変換機能を具備したＣＲＴ（Cathode-RayTube）装置のような、デジタル入力の表示装置とする。

【０１０２】図４において、上述した配布経路暗号化動作によって表示制御装置３０３の内部に展開されたデジタルコンテンツを含む表示データ（平文表示データ）は、ＣＰＵ３０１の指示に従って、表示メモリ３０４に蓄積される。

【０１０３】表示制御装置３０３においては、暗号処理

部４０１が、表示メモリ３０４に蓄積された平文表示データを入力し、入力した平文表示データの一部分に対して、表示制御装置３０３の内部に保持されている暗号鍵情報１０５を用いて暗号処理１０９を施し、表示制御装置３０３の内部に、暗号化された表示データを得る。得られた暗号化表示データは、表示制御装置３０３から表示装置１０３へ入力される。

【０１０４】続いて、表示装置１０３においては、復号処理部４０２が、入力した暗号化表示データ中の暗号化部分に対して、表示装置１０３の内部に保持されている暗号鍵情報１０５を用いて復号処理１１０を施し、表示装置１０３の内部に、平文表示データを得る。続いて、データドライバ４０３が、復号処理部４０２が復号した平文表示データを、表示画面上の各々の表示画素に供給することで、平文表示データの表示処理１１１を行う。

【０１０５】以上の動作が出力経路暗号化動作に相当している。

【０１０６】なお、暗号処理部４０２は、表示制御装置３０３内にハードウェアとして実装されるようにしてもよいし、また、表示制御装置３０３内に独自のＣＰＵおよびメモリを設け、ソフトウェアとして実装されるようにしてもよい。

【０１０７】次に、本実施形態に係る表示制御装置３０３の概略動作について、図８を用いて説明する。

【０１０８】図８は、本実施形態に係る表示制御装置３０３の概略構成図である。

【０１０９】図８では、表示制御装置３０３のうち、出力経路暗号化動作に関する部分のみを示している。

【０１１０】図中、８０１はメモリ制御部、８０２はタイミング生成部、８０３はタイミング信号、８０４はメモリ制御信号、８０５はメモリアドレス信号、３０４は表示メモリ、８０６はＬＣＤ制御部、８０７はＬＣＤ制御信号、８０８は平文表示データ、８０９はタイミング制御部、８１０はＬＣＤ表示データ、８１１はシリアル／パラレル変換回路（Ｓ／Ｐ回路）、８１２はＳ／Ｐ済ＬＣＤ表示データ、８１３は暗号化Ｓ／Ｐ済ＬＣＤ表示データ、８１４はパラレル／シリアル変換回路（Ｐ／Ｓ回路）、８１５は暗号化ＬＣＤ表示データ、８１６は遅延回路、８１７は遅延済ＬＣＤ制御信号である。

【０１１１】図８において、メモリ制御部８０１は、タイミング生成部８０２から送られてくるタイミング信号８０３を用いて、メモリ制御信号８０４およびメモリアドレス信号８０５を生成し、表示メモリ３０４から平文表示データ８０８を順次読み出す。

【０１１２】一方、ＬＣＤ制御部８０６は、タイミング生成部８０２から送られてくるタイミング信号８０３を用いて、ＬＣＤの表示タイミングを制御するＬＣＤ制御信号８０７を生成する。

【０１１３】タイミング制御部８０９は、表示メモリ３０４から読み出された平文表示データ８０９を、ＬＣＤ制御信号８０７による表示タイミングに合わせて、ＬＣＤ表示データ８１０として送り出す。

【０１１４】すなわち、表示メモリ３０４から読み出された平文表示データ８０８は、タイミング制御部８０９によって、ＬＣＤ制御信号８０７に同期したＬＣＤ表示データ８１０となる。

【０１１５】例えば、ＬＣＤ制御信号８０７が、１データ転送クロック同期で１画素分の表示データを転送し、かつ、１画素が１６ビットのデータから構成されているとすると、ＬＣＤ表示データ８１０は、１６ビットデータバスとなる。ここで、暗号処理に、例えば、ＤＥＳのようなブロック暗号を用いた場合、暗号処理部４０１は、暗号鍵情報１０５を用いて、６４ビット単位のブロック暗号処理を施すこととなる。

【０１１６】両者の処理単位の違いを吸収するために、本実施形態に係る表示制御装置３０３においては、Ｓ／Ｐ回路８１２およびＰ／Ｓ回路８１４を用いている。Ｓ／Ｐ回路８１１は、ＬＣＤ表示データ８１０のデータ幅（ここでは、１６ビット単位）を、暗号処理単位（ここでは、６４ビット単位）幅に変換し、Ｓ／Ｐ済ＬＣＤ表示データ８１２として暗号処理部４０１に供給するものであり、また、Ｐ／Ｓ回路８１４は、暗号処理部４０１によって暗号処理が施された後の暗号化Ｓ／Ｐ済ＬＣＤ表示データ８１３のデータ幅を、ＬＣＤ表示データ８１０のデータ幅に変換し、暗号化ＬＣＤ表示データ８１５としてデータドライバ４０３に供給するものである。

【０１１７】ＬＣＤ表示データ８１０のデータ幅と暗号処理部４０１の暗号処理単位幅とに応じて、Ｓ／Ｐ回路８１１およびＰ／Ｓ回路８１４の構成は異なる。

【０１１８】図８に示すように、本実施形態に係る表示制御装置３０３においては、Ｓ／Ｐ回路８１１，暗号処理部４０１，Ｐ／Ｓ回路８１４による処理が設けられているので、これらの処理による遅延と同等の遅延を、遅延回路８１６によって、ＬＣＤ制御部８０６が生成したＬＣＤ制御信号８０７に加え、遅延済ＬＣＤ制御信号８１７として出力するようにすることで、Ｐ／Ｓ回路８１４から出力される暗号化ＬＣＤ表示データ８１６が、遅延済ＬＣＤ制御信号８１７に同期してデータドライバ４０３に供給されるようにしている。

【０１１９】これにより、表示制御装置３０３による表示タイミング制御の処理途上で、表示データの一部分に対して暗号処理を施すこと、すなわち、ＬＣＤ表示データ８１０のリアルタイム暗号処理による暗号化ＬＣＤ表示データ８１５の作成が可能となる。

【０１２０】次に、本実施形態に係る表示装置１０３の概略動作について、図９を用いて説明する。

【０１２１】図９は、本実施形態に係る表示装置１０３の概略構成図である。

【０１２２】図９では、表示装置１０３が液晶表示装置である場合を例にしており、表示装置１０３のうち、出

力経路暗号化動作に関する部分（すなわち、データドライバ４０３に相当する液晶駆動ドレイン側ドライバ）のみを示している。

【０１２３】図中、９０１は暗号化表示データの取り込み信号（ＣＬ２信号）、９０２は暗号化表示データ、９０３はＬＣＤ駆動電圧を出力するタイミング信号（ＣＬ１信号）、９０４はＬＣＤ駆動用電源、９０５は液晶駆動出力信号、９０６はラッチアドレスセレクタ、９０７はラッチ回路－１、９０８はラッチ回路－２、９０９は回路駆動電圧から液晶駆動電圧へ昇圧するレベルシフタ、９１０は液晶駆動用の電圧レベルを発生する液晶駆動回路、９１１はラッチ回路－３、９１２は平文表示データである。

【０１２４】図９において、ラッチアドレスセレクタ９０６は、暗号化表示データ９０２の入力と同期して表示制御装置３０３から入力したＣＬ２信号９０１（図８に示した遅延済ＬＣＤ制御信号８１７に相当している。）の立下りをカウントすることで、ラッチ回路－１（９０７）に対するラッチ信号を生成する。

【０１２５】表示制御装置３０３から入力した暗号化表示データ９０２は、ラッチアドレスセレクタ９０６が生成するラッチ信号によって、ラッチ回路－１（９０７）上に入力順に保持されていく。

【０１２６】ＣＬ１信号９０３は、表示１ラインごとに入力する水平同期信号であり、ＣＬ１信号９０３の入力によって、ラッチ回路－１（９０７）上にラッチされた１表示ライン分の暗号化表示データ９０２は、１ライン表示期間ごとに、１ライン分ずつ、ラッチ回路－２（９０８）上にラッチされる。

【０１２７】ラッチ回路－２（９０８）上にラッチされた１ライン分の暗号化表示データ９０２は、復号処理部４０２によって、暗号鍵情報１０５を用いた復号処理１００が施されて平文表示データ９１２となり、ＣＬ１信号９０３によって、１ライン表示期間ごとに、１ライン分ずつ、ラッチ回路－３（９１１）上にラッチされる。

【０１２８】ラッチ回路－３（９１１）上にラッチされた１ライン分の平文表示データ９１２は、レベルシフタ９０９および液晶駆動回路９１０を介して液晶駆動電圧に変換され、１ライン表示期間、液晶に印加される。

【０１２９】以上の処理により、１ラインごとに液晶への表示動作が実行される。

【０１３０】ここで、復号処理に、例えば、ＤＥＳのようなブロック暗号を用いた場合、復号処理部４０２は、ラッチ回路－２（９０８）から出力されるビット数を、同時に並列処理可能な分だけ、ブロック単位に並列させる。例えば、液晶駆動ドレイン側ドライバが、１ライン当たり１０２４画素構成で１画素当たり１８ビット出力であるとすると、１ライン当たり１８４３２ビットとなるので、６４ビット単位（ＤＥＳによる処理単位）のブロックを２８８個並列させる。そして、復号処理部４０２は、暗号鍵情報１０５を用いて、６４ビット単位のブロック復号処理を施すこととなる。

【０１３１】これにより、表示装置１０３の液晶駆動ドレイン側ドライバによる表示制御の処理途上で、表示データの一部分に対して復号処理を施すこと、すなわち、暗号化表示データ９１２のリアルタイム復号処理による平文表示データ９１２の作成・表示が可能となる。

【０１３２】なお、本実施形態に係る表示装置１０３は、図９に示す構成ではなく、図１０に示す構成にしてもよい。

【０１３３】図１０は、本実施形態に係る表示装置１０３の他の概略構成図である。

【０１３４】図１０でも、図９と同様に、表示装置１０３が液晶表示装置である場合を例にしており、表示装置１０３のうち、出力経路暗号化動作に関する部分（すなわち、データドライバ４０３に相当する液晶駆動ドレイン側ドライバ）のみを示している。

【０１３５】図中、図９と同じ構成要素には同じ符号を付与してある。１００１はＳ／Ｐ回路、１００２はＰ／Ｓ回路、１００３はＳ／Ｐ済表示データ、１００４は平文表示データである。

【０１３６】図１０に示す表示装置１０３は、暗号化表示データ９０２のデータ幅が、１画素当たりのデータビット数とデータ転送クロック（ＣＬ２信号９０１）とに依存し、復号処理部４０２の復号処理単位のデータ幅と異なっている場合に、Ｓ／Ｐ回路１００１によって、暗号化表示データ９０２のデータ幅を適切な復号処理単位のデータ幅に変換し、Ｓ／Ｐ済表示データ１００３としてから、復号処理部４０２によって、暗号鍵情報１０５を用いて復号処理を行い、復号処理によって得られた平文表示データ１００４を、Ｐ／Ｓ回路１００２によって、平文表示データ９１２のデータ幅に変換するようにしたものである。

【０１３７】復号処理部４０２は、最低１ブロックを処理できればよく、１画素当たりの暗号化表示データ９０２のビット数とＣＬ２信号９０１とに応じて、処理ブロックを並列させるようにしてもよい。

【０１３８】以上、表示装置１０３が液晶表示装置である場合を例にとって、出力経路暗号化動作について説明したが、表示装置１０３が、例えば、デジタル入力でデジタル／アナログ変換部を具備するＣＲＴ装置である場合でも、デジタル処理を行う途上で、同様の復号処理を行うようにすれば、平文表示データの作成・表示が可能となる。

【０１３９】次に、出力経路暗号化動作で、表示制御装置３０３から出力される表示データの暗号化方法の一例について、図１１および図１２を用いて説明する。

【０１４０】図１１は、表示制御装置３０３から出力される表示データの暗号化方法の一例を示す説明図であり、暗号化された表示データを表示装置１０３で表示し

た場合の表示イメージを示す説明図である。

【０１４１】図１１では、元画像（本来の平文表示データ）の暗号化方法として、ライン方向に暗号処理を施す暗号化方法と、カラム方向に暗号処理を施す暗号化方法とを示している。

【０１４２】（１）ライン方向に暗号処理を施す暗号化方法

例えば、図１１（ａ）に示す元画像（本来の平文表示データ）に対して、本方法による暗号化を行う際には、ライン方向に、複数ライン分（例えば、数ライン程度）の表示データを１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すようにする。具体的には、数ライン分の表示データごとに、交互に、暗号処理を施す場合と暗号処理を施さない場合とを繰り返すようにする。

【０１４３】本方法により暗号化された表示データは、暗号鍵情報１０５を用いた復号処理を施せば、表示装置１０３に表示される際のイメージは、図１１（ａ）に示す元画像と同じイメージになるが、暗号鍵情報１０５を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図１１（ｂ）に示すように、数ラインおきに数ライン分が汚損された表示データとなる。

【０１４４】本方法では、１単位とするライン数を予め決定しておき、決定したライン数ごとに、表示制御装置３０３の暗号処理部４０１が選択的に暗号化すると共に、表示装置１０３の復号処理部４０２が選択的に復号するようにする。これにより、表示データの一部に対する汚損が可能となり、また、表示制御装置３０３の暗号処理部４０１および表示装置１０３の復号処理部４０２における暗号／復号処理量の削減が可能となる。

【０１４５】また、１単位とするライン数を増減させることで、表示データの汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【０１４６】（２）カラム方向に暗号処理を施す暗号化方法

例えば、図１１（ａ）に示す元画像（本来の平文表示データ）に対して、本方法による暗号化を行う際には、カラム方向に、複数カラム分（例えば、数カラム程度）の表示データを１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すようにする。具体的には、数カラム分の表示データごとに、交互に、暗号処理を施す場合と暗号処理を施さない場合とを繰り返すようにする。

【０１４７】本方法により暗号化された表示データは、暗号鍵情報１０５を用いた復号処理を施せば、表示装置１０３に表示される際のイメージは、図１１（ａ）に示す元画像と同じイメージになるが、暗号鍵情報１０５を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図１１（ｃ）に示すように、数カラムおきに数カラム分が汚損された表示データとなる。

【０１４８】本方法では、１単位とするカラム数を予め決定しておき、決定したカラム数ごとに、表示制御装置３０３の暗号処理部４０１が選択的に暗号化すると共に、表示装置１０３の復号処理部４０２が選択的に復号するようにする。これにより、表示データの一部に対する汚損が可能となり、また、表示制御装置３０３の暗号処理部４０１および表示装置１０３の復号処理部４０２における暗号／復号処理量の削減が可能となる。

【０１４９】また、１単位とするカラム数を増減させることで、表示データの汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【０１５０】図１２は、表示制御装置３０３から出力される表示データの暗号化方法の一例を示す説明図であり、図１２では、元画像（本来の平文表示データ）中の１画素分の表示データについて、その一部分に対して暗号処理を施す暗号化方法を示している。

【０１５１】本方法では、１画素内の表示データ中の上位ビットのみに暗号処理を施すようにするか、または、１画素内の表示データ中の下位ビットのみに暗号処理を施すようにする。

【０１５２】上位ビットのみを暗号化し、下位ビットは平文のままとした場合は、表示データの変化量が大きくなる。そこで、暗号化表示データを復号せずに表示装置１０３上で表示すると、データの汚損度が大きく、表示データの観察は困難となる。

【０１５３】また、下位ビットのみを暗号化し、上位ビットは平文のままとした場合は、表示データの変化量は少ない。そこで、暗号化表示データを復号せずに表示装置１０３上で表示すると、データの汚損度が小さく、画面上のちらつきとして観察されるが、表示データのおおまかな観察は可能である。

【０１５４】図１２では、１画素分の表示データが８ビットで構成され、ある平文表示データが「５５ｈ」であるとしたときに、上位ビットのみを暗号化して「５５ｈ」が「ｅ５ｈ」になり、下位ビットのみを暗号化して「５５ｈ」が「５２ｈ」になった例を示した。このように、上位ビットのみを暗号化する方が、平文表示データからの変化量が大きくなるので、より異なった表示として観測されることとなる。

【０１５５】本方法では、上位ビットのみを暗号化するか、または、下位ビットのみを暗号化するかを選択することで、表示データの汚損度合を選択することが可能であり、また、表示制御装置３０３の暗号処理部４０１および表示装置１０３の復号処理部４０２における暗号／復号処理量の削減が可能となる。

【０１５６】以上、ライン方向／カラム方向に暗号処理を施す暗号化方法、および、１画素内の表示データ中の上位ビット／下位ビットのみに暗号処理を施す暗号化方

法について説明したが、これらの方法を任意に組み合わせるようにしてもよい。

【０１５７】本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作によって、従来は行われていなかった、最終出力装置である表示装置１０３への出力経路でのデジタルコンテンツの著作権保護が可能となる。

【０１５８】そして、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作において、デジタルコンテンツ（表示データ）を単純に暗号化するのではなく、暗号処理の処理対象とするデータを選択し、一部分のみを暗号化するようにしているので、正当な暗号鍵情報１０５を有していない場合には、元画像の一部分が汚損した状態となる。一部分が汚損されたデジタルコンテンツは、その価値が損なわれるので、デジタルコンテンツの不正コピーを防止することが可能となり、また、デジタルコンテンツの一部分が開示されるので、ユーザの視聴要求を刺激し、デジタルコンテンツの完全な視聴を促すことが可能となる。

【０１５９】さらに、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作において、デジタルコンテンツの一部分だけを暗号処理の処理対象とし、デジタルコンテンツ全体に対する暗号処理を避けることによって、暗号処理／復号処理の処理量の軽減も可能となっている。なお、汚損度と処理量とはトレードオフの関係にあり、要求に応じて優先度の変更が容易に可能である。

【０１６０】以上説明したように、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作によって、デジタルコンテンツの出力経路上で著作権を保護しつつ、ユーザの視聴欲求を刺激することが可能となる。

【０１６１】なお、本実施形態に係る情報処理装置１０１は、図４に示す構成ではなく、図１３に示す構成にし、図４に示した暗号処理部４０１を、ソフトウェアで実現するようにしてもよい。

【０１６２】図１３は、本実施形態に係る情報処理装置１０１の他の概略構成図である。

【０１６３】図１３でも、図４と同様に、ＰＣなどの情報処理装置１０１のうち、表示に関する部分であって、かつ、出力経路暗号化動作に関する部分のみを示している。

【０１６４】図中、図４と同じ構成要素には同じ符号を付与してある。７０１は不揮発性記憶装置である。

【０１６５】図１３に示す構成の情報処理装置１０１においては、図４に示した暗号処理部４０１の動作を、ＣＰＵ３０１がシステムメモリ３０２上にプログラムをロードして実行することで実現するものである。すなわち、図１３に示す構成の情報処理装置１０１は、表示制御装置３０３ではなく、ＣＰＵ３０１が表示データを暗号化するようにしている。

【０１６６】図１４は、図１３に示す構成の情報処理装置１０１の概略動作を示す説明図である。

【０１６７】図１４に示すように、表示メモリ３０４に蓄積された平文表示データ８０８は、ＣＰＵ３０１の指示に従って、表示制御装置３０３およびバス３０７を介してシステムメモリ３０２に入力される。

【０１６８】ＣＰＵ３０１は、入力した平文表示データ８０８に対して、暗号鍵情報１０５を用いて暗号処理１０９を施す。ＣＰＵ３０１によって暗号化された暗号化表示データ９０２は、バス３０７および表示制御装置３０３を介して表示メモリ３０４にに入力される。表示メモリ３０４に蓄積された暗号化表示データ９０２は、表示制御装置３０３によって読み出され、表示装置１０３に出力される。

【０１６９】すなわち、図１３に示す構成の情報処理装置１０１においては、ＣＰＵ３０１が、表示メモリ３０４上に平文表示データ８０８を生成し、さらに、平文表示データ８０８から表示メモリ３０４上に暗号化表示データ９０２を生成する。表示制御装置３０３は、暗号化表示データ９０２の読み出し動作を行い、表示動作を行う。

【０１７０】ここで、暗号鍵情報１０５は、図４を用いた説明では、表示制御装置３０３の内部に保持されているものとしたが、図１３に示す構成の情報処理装置１０１においては、暗号鍵情報１０５は、不揮発性記憶装置７０１に保持されているものとする。

【０１７１】また、本実施形態に係る情報処理装置１０１は、図４および図１３のいずれにおいても、情報処理装置１０２本体と表示装置１０３とを備えた構成としているが、配布経路暗号化動作で説明したのと同様に、情報処理装置本体１０２と表示装置１０３が一体化した構成であってもよい。すなわち、本実施形態に係る情報処理装置１０１を、いわゆるＰＤＡなどと呼ばれる携帯情報端末としてもよい。

【０１７２】上述したように、一般に、携帯情報端末は、比較的性能の低いＣＰＵや小容量のメモリなどを用いて構成されることが多いので、比較的重い処理である暗号処理は携帯情報端末にとって大きな負担になるという問題がある。

【０１７３】そこで、このような問題がある携帯情報端末を、本実施形態に係るデジタルコンテンツ配布システムで用いるようにすれば、全体ではなく一部分が暗号化されたデジタルコンテンツを扱うことにより、本発明が目的とする、著作権保護とユーザの視聴覚欲求刺激の両立を実現することができる上、暗号処理量の低減による負荷低下効果を得ることができる。特に、携帯情報端末が暗号処理をソフトウェアで実現する場合には、暗号処理用に高性能なＣＰＵや大容量メモリを搭載する必要がなくなり、低コスト化，低消費電力化といった効果が得

られる。また、携帯情報端末が暗号処理専用のハードウェアを備えるようにする場合には、暗号処理専用のハードウェアに必要な処理速度が低下することから、低動作速度による低消費電力化，ハードウェア論理の小規模化による低コスト化といった効果が得られる。

【０１７４】ところで、上述の説明では、デジタル表示装置への出力を例にしたが、必ずしも表示のみを対象としている訳ではない。

【０１７５】例えば、デジタル入力を持った音声出力装置においても、ＰＣＭ（Pulse CodeModulation）符号化された音声データに対して、同様に、数サンプルおきに暗号化を施すことで、出力装置経路暗号化動作を実現することが可能である。

【０１７６】以上説明したように、本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツのフォーマットに依存する形で、デジタルコンテンツの一部分に対して暗号処理を施すようにすることで、正当な暗号鍵情報を有さない場合に、一部が汚損されたデジタルコンテンツとなるようにしている。そこで、デジタルコンテンツの著作権を保護しつつ、ユーザの視聴覚欲求を刺激することが可能となる。

【０１７７】従って、本実施形態に係るデジタルコンテンツ配布システムによれば、付加価値の高いデジタルコンテンツを，安全に半導体記憶媒体やデジタルネットワーク上で流通させることが可能となり、デジタルコンテンツ配布サービスなどへの応用が可能となる。

【０１７８】なお、デジタルコンテンツの保護においては、配布経路暗号化動作および出力経路暗号化動作のうちのいずれか一方を用いたシステムとしてもよいし、また、両者を組み合わせ、２つの独立した暗号方式によって、デジタルコンテンツの保護を行うシステムとしてもよい。

【０１７９】

【発明の効果】以上説明したように、本発明によれば、デジタルコンテンツの著作権を保護しつつ、ユーザの視聴覚欲求を刺激することの可能な、デジタルコンテンツの最終出力が可能となる。

【図面の簡単な説明】

【図１】本実施形態に係るデジタルコンテンツ配布システムの概略構成図。

【図２】本実施形態に係るデジタルコンテンツ配布システムの概略動作フローチャート。

【図３】本実施形態に係る情報処理装置の概略構成図。

【図４】本実施形態に係る情報処理装置の概略構成図。

【図５】デジタルコンテンツ配布装置から配布されるデジタルコンテンツの暗号化方法の一例を示す説明図。

【図６】図５に示す暗号化方法で暗号化されたデジタルコンテンツを表示装置で表示した場合の表示イメージを示す説明図。

【図７】本実施形態に係る情報処理装置の概略構成図。

【図８】本実施形態に係る表示制御装置の概略構成図。

【図９】本実施形態に係る表示装置の概略構成図。

【図１０】本実施形態に係る表示装置の概略構成図。

【図１１】表示制御装置から出力される表示データの暗号化方法の一例を示す説明図。

【図１２】表示制御装置から出力される表示データの暗号化方法の一例を示す説明図。

【図１３】本実施形態に係る情報処理装置の概略構成図。

【図１４】図１３に示した情報処理装置の概略動作を示す説明図。

【符号の説明】

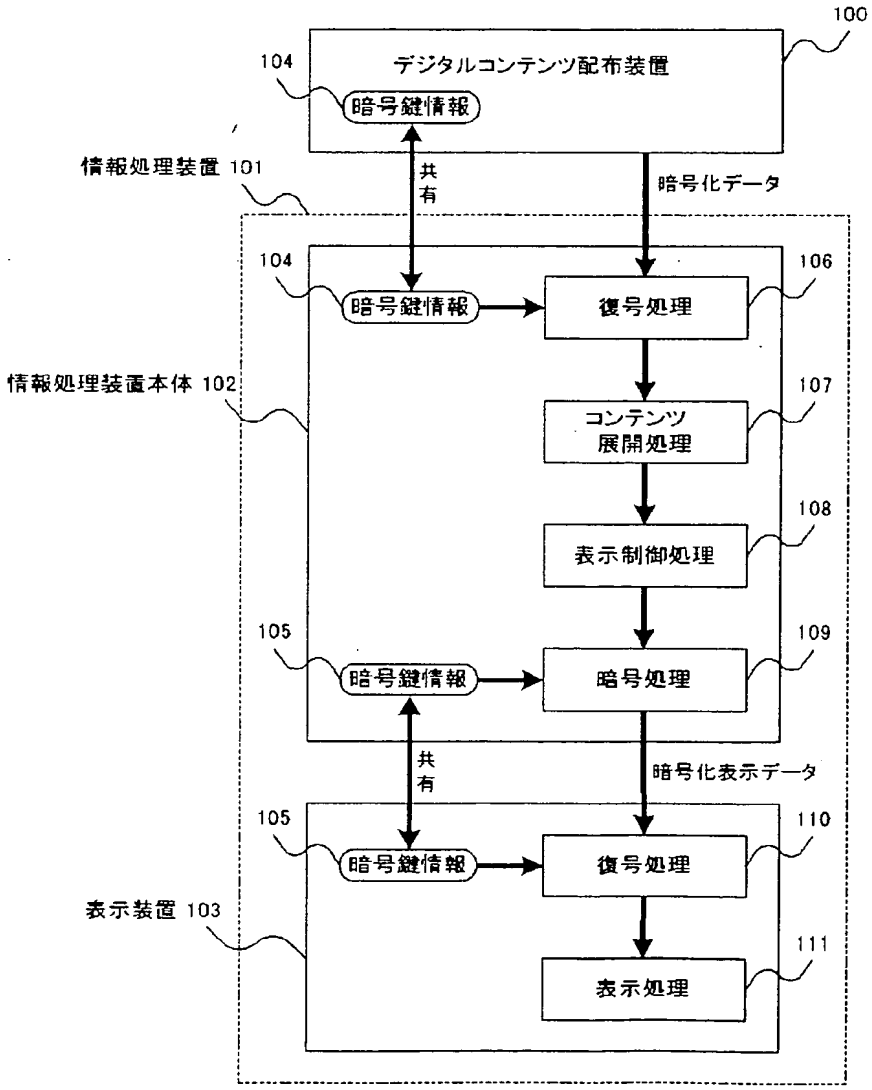
１００：デジタルコンテンツ配布装置
１０１：情報処理装置
１０２：情報処理装置本体
１０３：表示装置
１０４：暗号鍵情報
１０５：暗号鍵情報
１０６：復号処理
１０７：コンテンツ展開処理
１０８：表示制御処理
１０９：暗号処理
１１０：復号処理
１１１：表示処理
３０１：中央演算装置（ＣＰＵ：Central Processing Unit）
３０２：システムメモリ
３０３：表示制御装置
３０４：表示メモリ
３０５：入力制御装置
３０６：通信制御装置
３０７：バス
３０８：復号処理部
３０９：コンテンツ展開処理部
４０１：暗号処理部
４０２：復号処理部
４０３：データドライバ
７０１：不揮発性記憶装置
８０１：メモリ制御部
８０２：タイミング生成部
８０３：タイミング信号
８０４：メモリ制御信号
８０５：メモリアドレス信号
８０６：ＬＣＤ（Liquid Crystal Display）制御部
８０７：ＬＣＤ制御信号
８０８：平文表示データ
８０９：タイミング制御部
８１０：ＬＣＤ表示データ
８１１：シリアル／パラレル変換回路（Ｓ／Ｐ回路）
８１２：Ｓ／Ｐ済ＬＣＤ表示データ

27　　28

８１３：暗号化Ｓ／Ｐ済ＬＣＤ表示データ
８１４：パラレル／シリアル変換回路（Ｐ／Ｓ回路）
８１５：暗号化ＬＣＤ表示データ
８１６：遅延回路
８１７：遅延済ＬＣＤ制御信号
９０１：ＣＬ２信号
９０２：暗号化表示データ
９０３：ＣＬ１信号
９０４：ＬＣＤ駆動用電源
９０５：液晶駆動出力信号
９０６：ラッチアドレスセレクタ
＊９０７：ラッチ回路－１
９０８：ラッチ回路－２
９０９：レベルシフタ
９１０：液晶駆動回路
９１１：ラッチ回路－３
９１２：平文表示データ
１００１：Ｓ／Ｐ回路
１００２：Ｐ／Ｓ回路
１００３：Ｓ／Ｐ済表示データ
１００４：平文表示データ

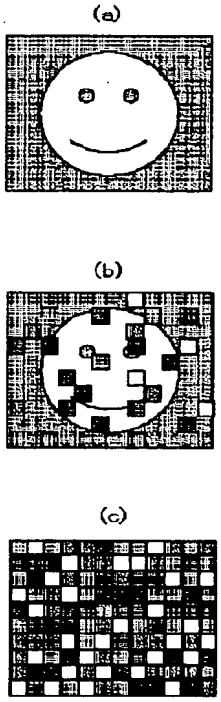
【図１】

図 1



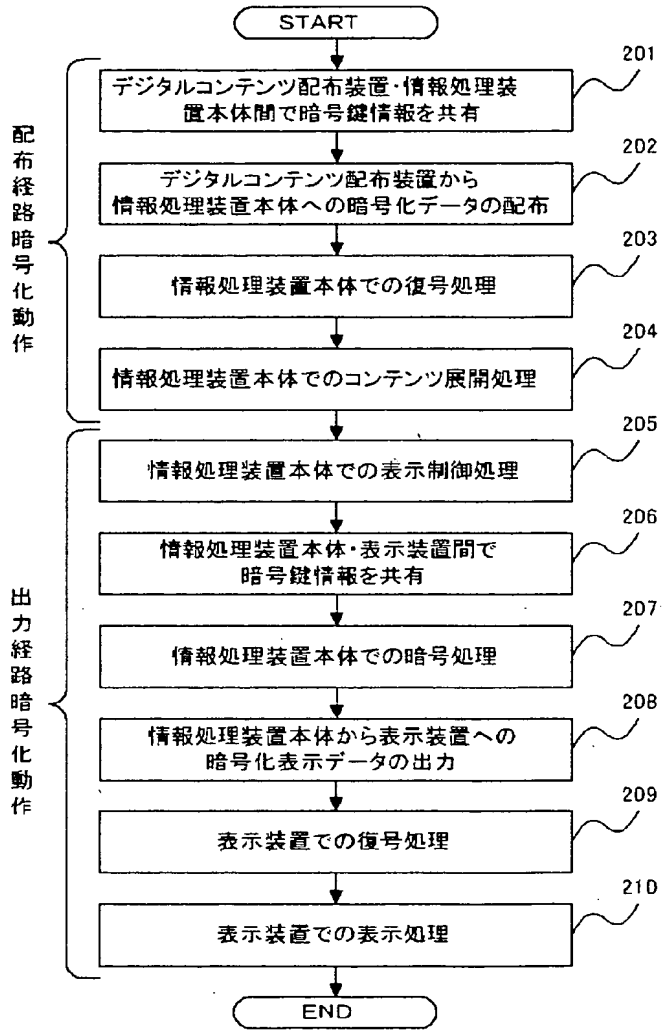
【図６】

図6



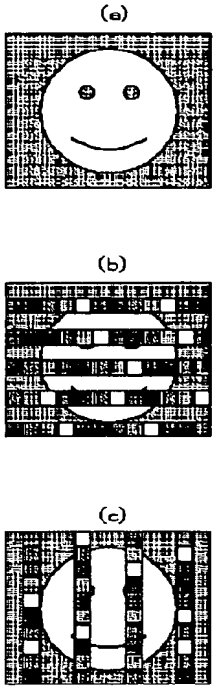
【図２】

図 2



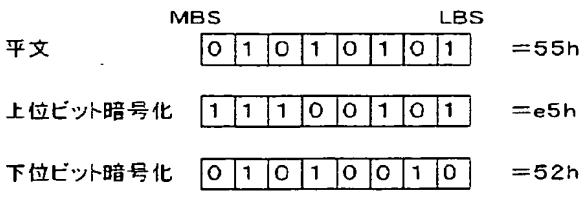
【図１１】

図11



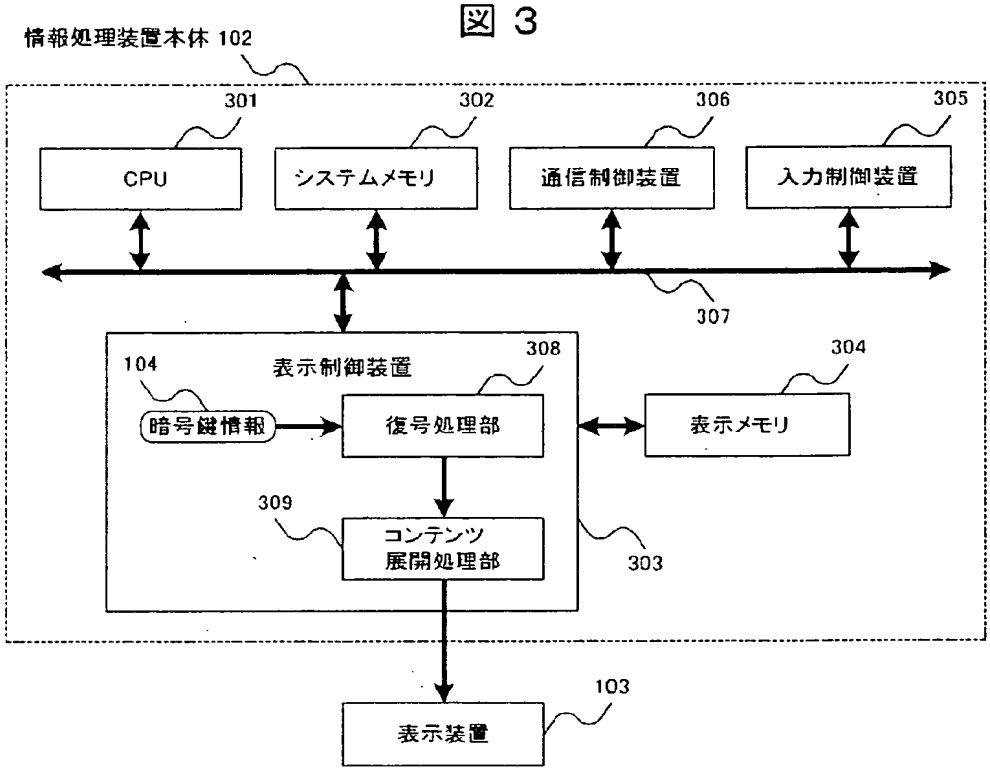
【図１２】

図 12



【図３】

図 3



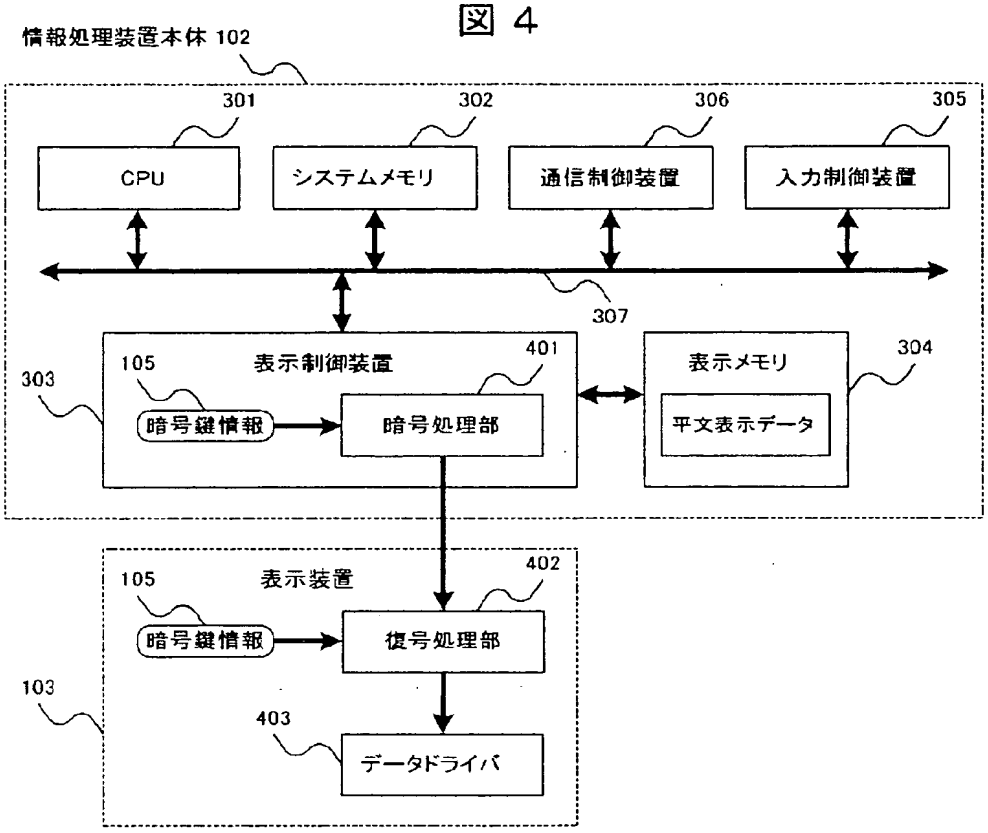
【図５】

図 5

暗号化対象	暗号鍵情報なしに得られるピクチャデータ			符号割り当て量@ピクチャデータ	暗号処理量@ピクチャデータ
	I	P	B		
Iピクチャデータ	×	×	×	大	大
Pピクチャデータ	○	×	×	中	中
Bピクチャデータ	○	○	×	小	小

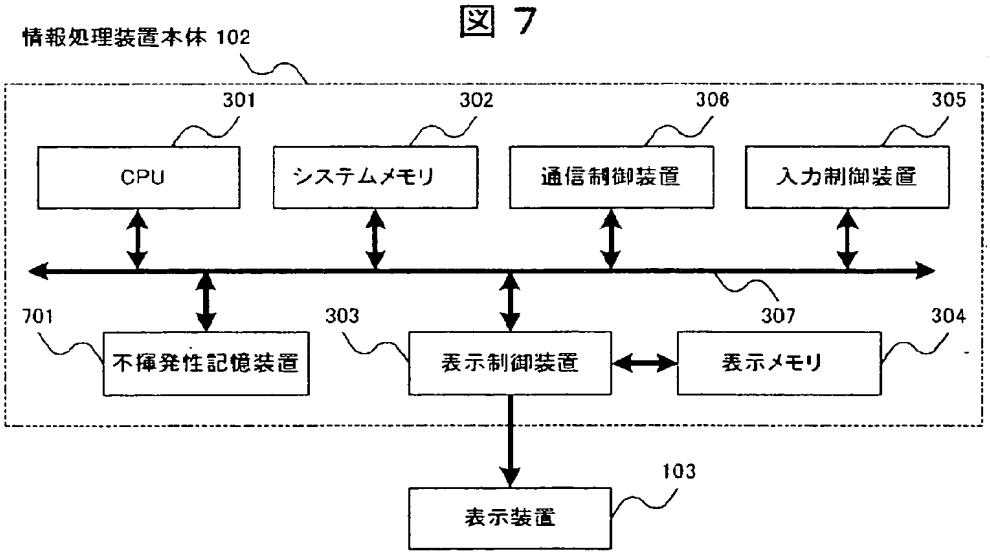
【図４】

図 4


情報処理装置本体 102
301
302
306
305
CPU
システムメモリ
通信制御装置
入力制御装置
307
105
表示制御装置
401
303
暗号鍵情報
暗号処理部
表示メモリ
304
平文表示データ
105
表示装置
402
暗号鍵情報
復号処理部
103
403
データドライバ

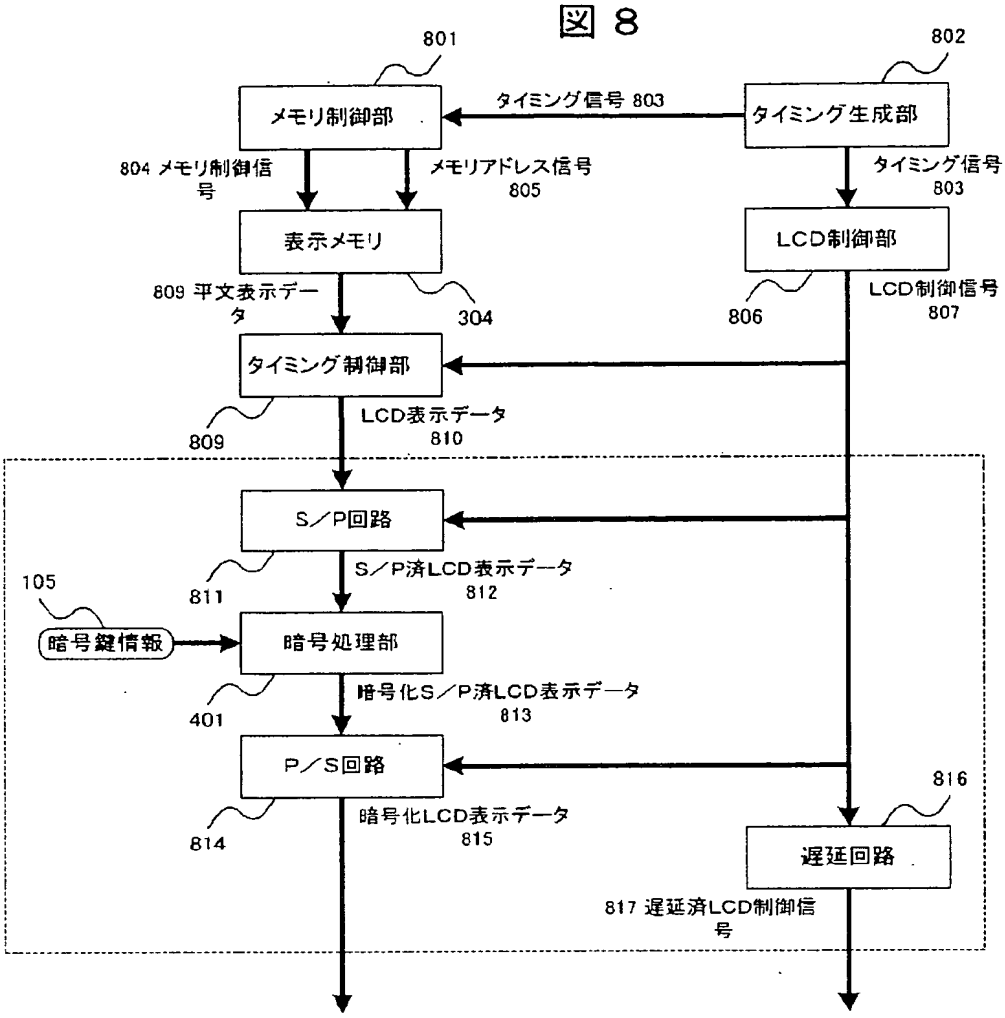
【図７】

図 7


情報処理装置本体 102
301
302
306
305
CPU
システムメモリ
通信制御装置
入力制御装置
307
701
303
304
不揮発性記憶装置
表示制御装置
表示メモリ
103
表示装置

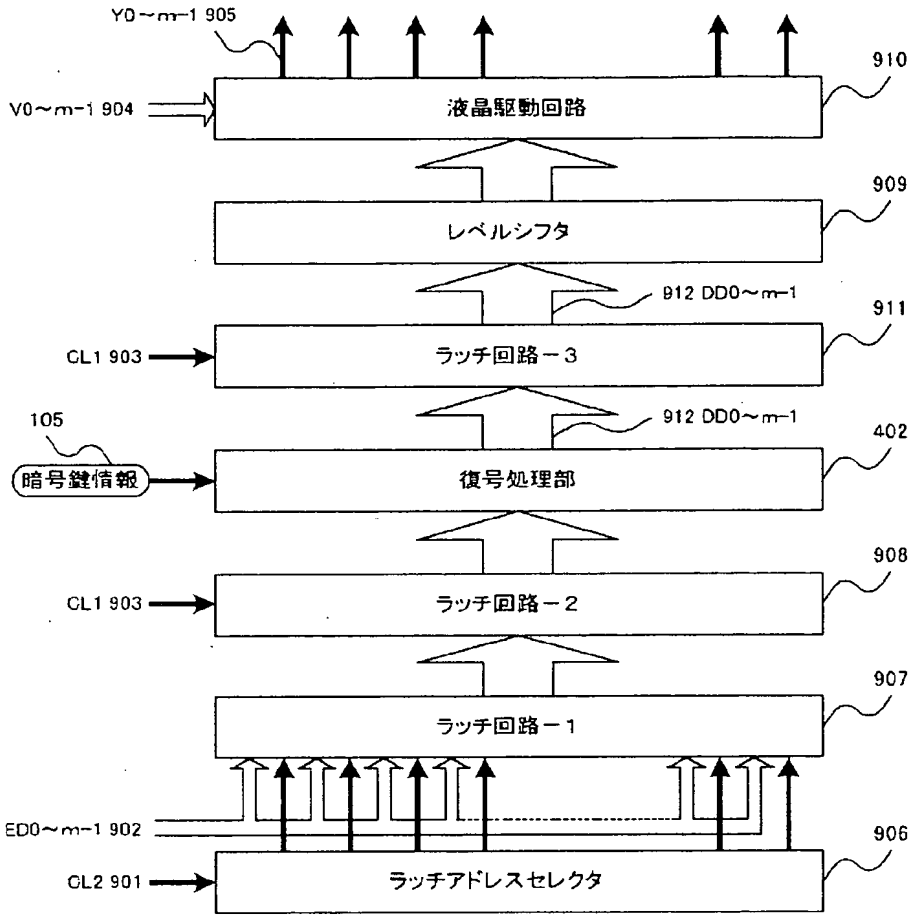
【図８】

図 8


801
802
メモリ制御部
タイミング信号 803
タイミング生成部
804 メモリ制御信号
メモリアドレス信号 805
タイミング信号 803
表示メモリ
LCD制御部
809 平文表示データ
304
806
LCD制御信号 807
タイミング制御部
809
LCD表示データ 810
S／P回路
811
S／P済LCD表示データ 812
105
暗号鍵情報
暗号処理部
401
暗号化S／P済LCD表示データ 813
P／S回路
814
暗号化LCD表示データ 815
816
遅延回路
817 遅延済LCD制御信号

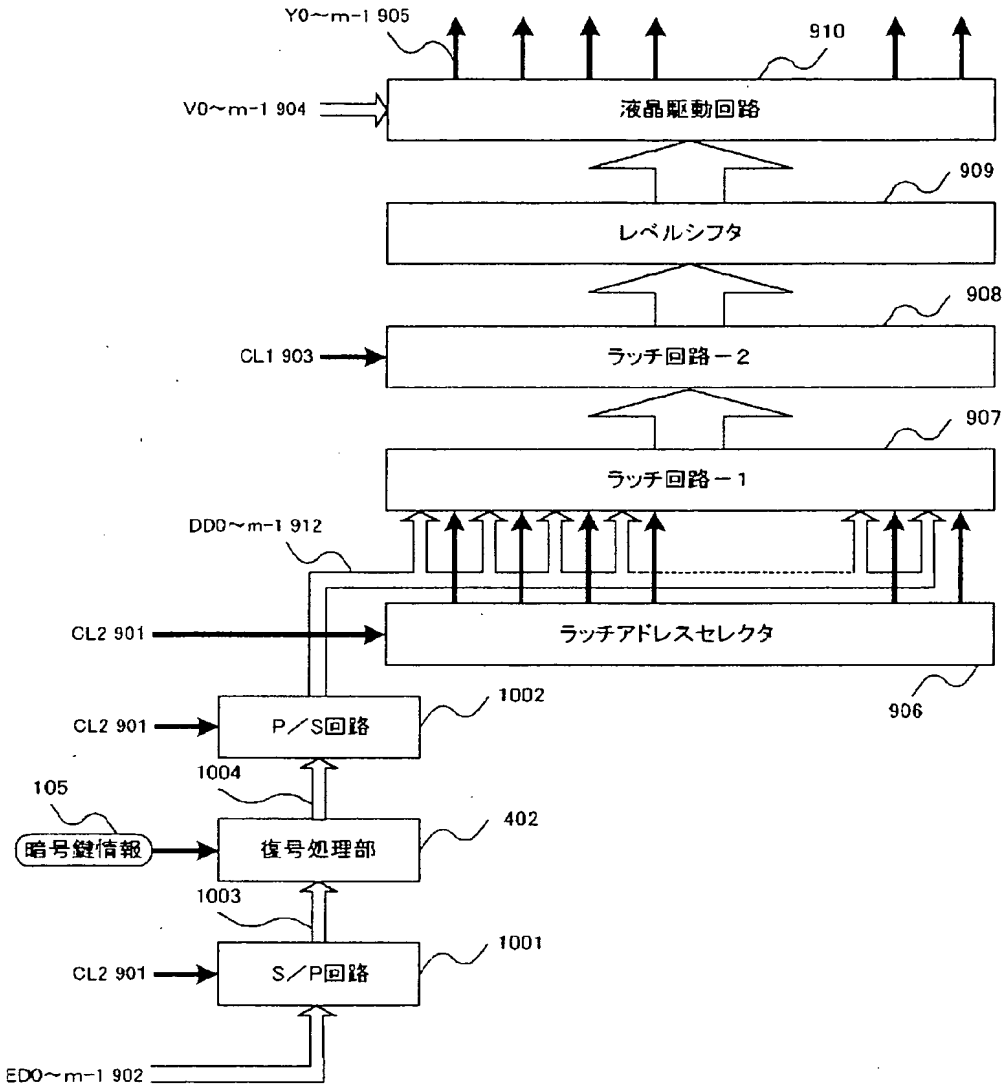
【図９】

図９


Y0～m-1 905
910
液晶駆動回路
V0～m-1 904
909
レベルシフタ
912 DD0～m-1
911
CL1 903
ラッチ回路－３
912 DD0～m-1
105
暗号鍵情報
402
復号処理部
908
CL1 903
ラッチ回路－２
907
ラッチ回路－１
ED0～m-1 902
906
CL2 901
ラッチアドレスセレクタ

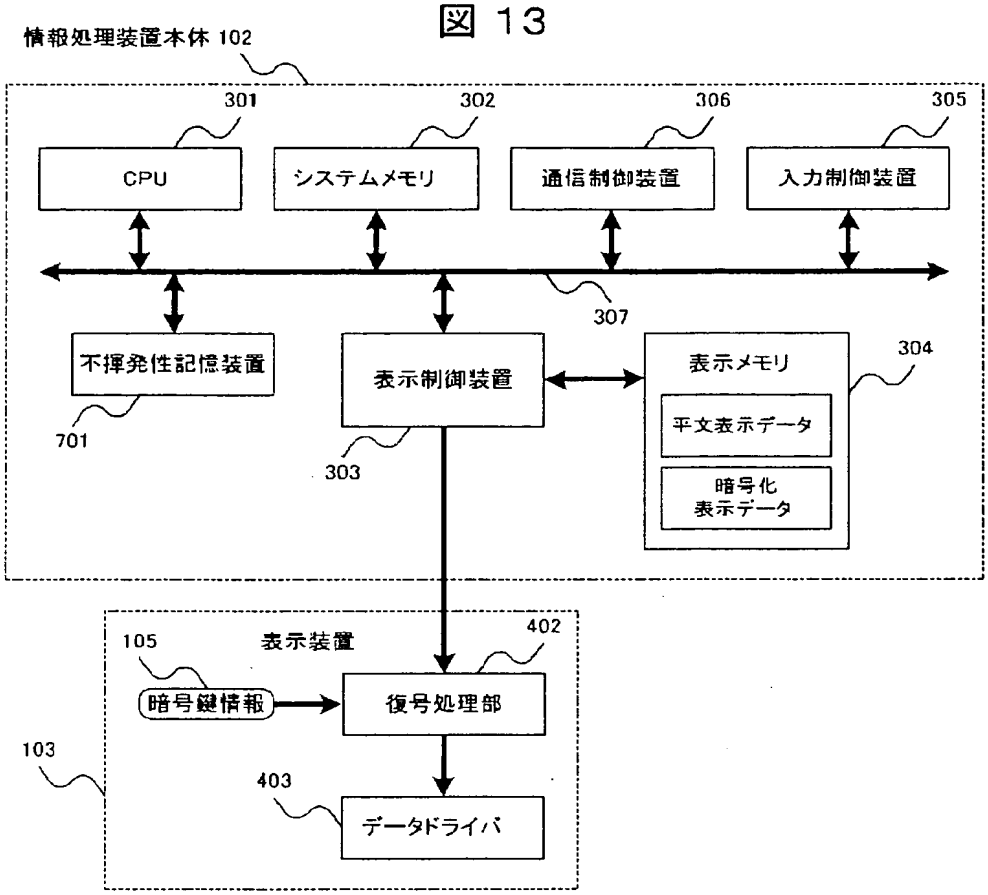
【図１０】

図 10


Y0～m-1 905
910
V0～m-1 904
液晶駆動回路
909
レベルシフタ
908
CL1 903
ラッチ回路－2
907
ラッチ回路－1
DD0～m-1 912
CL2 901
ラッチアドレスセレクタ
906
CL2 901
P／S回路
1002
1004
105
暗号鍵情報
復号処理部
402
1003
CL2 901
S／P回路
1001
ED0～m-1 902

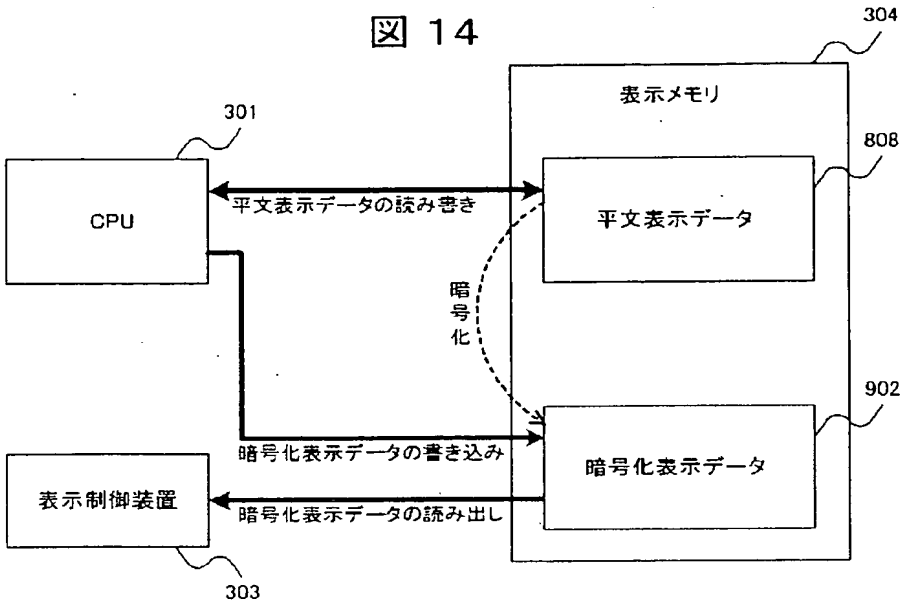
【図１３】

図 13


情報処理装置本体 102
301
302
306
305
CPU
システムメモリ
通信制御装置
入力制御装置
307
不揮発性記憶装置
701
表示制御装置
303
表示メモリ
304
平文表示データ
暗号化
表示データ
105
表示装置
402
暗号鍵情報
復号処理部
103
403
データドライバ

【図１４】

図 14



フロントページの続き

(72)発明者　朝日　猛
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

Ｆターム(参考)　5C064 CA18
5J104 AA34 AA37 AA39 DA02 EA02 EA04 JA03 NA02